ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Υπολογιστικό Νέφος & Ηλεκτρονικές Ταυτότητες: Προβλήματα Ιδιωτικότητας

ΡΟΖΑΛΙΑ ΚΑΛΑΝΤΖΗ

Μ.Δ.Ε: Υπολογιστικά Μαθηματικά – Πληροφορική στην Εκπαίδευση
Κατεύθυνση: Τεχνολογίες Πληροφορικής & Επικοινωνιών στην Εκπαίδευση

Επιβλέπων: Γ. Μητακίδης, Καθηγητής

Πάτρα, Ιούνιος 2011

Ευχαριστίες

Νοιώθω την ανάγκη να ευχαριστήσω θερμά τον Καθηγητή κ. Γεώργιο Μητακίδη ο οποίος επέβλεψε την παρούσα διπλωματική εργασία. Με καθοδήγησε με μεθοδικότητα, υπομονή και στοχευμένες συμβουλές. Με την πολύτιμη βοήθειά του ξεπεράστηκαν οι όποιες δυσκολίες προέκυψαν και κατάφερα να πετύχω τον στόχο μου. Αποτελεί ιδιαίτερη τιμή για μένα που μου εμπιστεύτηκε το θέμα που πραγματεύεται η εργασία καθώς και που υπήρξα φοιτήτριά του. Επίσης θα ήθελα να τον ευχαριστήσω για τις πολύ ενδιαφέρουσες συζητήσεις μας όπως επίσης και για όλα όσα μου δίδαξε καθ' όλη την διάρκεια των σπουδών μου.

Παράλληλα από την θέση αυτή θα ήθελα να ευχαριστήσω τον Επίκουρο Καθηγητή κ. Ιωάννη Σταματίου για την σημαντική συμβολή του. Υπήρξε σύμβουλος, συνεργάτης και υποστηρικτής της προσπάθειάς μου σε βαθμό μεγαλύτερο από το προβλεπόμενο, γι' αυτό και τον ευχαριστώ θερμά.

Επιπλέον, θα επιθυμούσα να εκφράσω την ευγνωμοσύνη μου στον Επίκουρο Καθηγητή κ. Δημήτριο Καββαδία ο οποίος μου έκανε τη τιμή να συμμετάσχει στην τριμελή εξεταστική επιτροπή της διπλωματικής εργασίας μου.

Τέλος, μέσα από την καρδία μου ευχαριστώ στην οικογένειά μου, ειδικότερα στην μητέρα μου για την υπομονή που έδειξε στηρίζοντάς με καθ' όλη την διάρκεια των σπουδών μου και για την ενθάρρυνση της χάρη στην οποία κατάφερα να αντιμετωπίσω όλα τα προβλήματα που συνάντησα.

Περίληψη

Η *ιδιωτικότητα (privacy)* είναι μια λέξη που ακούμε πολύ συχνά στις μέρες μας. Παρόλα αυτά δεν είναι εύκολο να διατυπώσει κανείς έναν αυστηρό ορισμό. Γενικά, είναι η μέριμνα ενός ατόμου ή μιας ομάδας ατόμων να προστατεύουν πληροφορίες σχετικές με αυτούς και όσες αυτοί θέλουν ή όσες επιβάλλονται από την κοινωνία ή και την πολιτεία, και έτσι να «αποκαλύπτονται» επιλεκτικά. Τα όρια και το περιεχόμενο του τι θεωρείται ιδιωτικό διαφέρει μεταξύ πολιτισμών, χωρών και διαφορετικών ατόμων, αλλά μοιράζεται βασικά κοινά θέματα. Όσο αφορά τον χώρο της Πληροφορικής, *ιδιωτικότητα της πληροφορίας* (information privacy) ή *ιδιωτικότητα των δεδομένων* (data privacy) είναι η συσχέτιση ανάμεσα στην συλλογή και διάδοση των δεδομένων, στην τεχνολογία, στην προσδοκία της κοινωνίας για ιδιωτικότητα και στα νομικά ζητήματα που περιβάλλουν όλα αυτά.

Η ιδιωτικότητα αποτελεί κεντρικό θέμα στον Παγκόσμιο Ιστό (Web). Τέμνει θέματα όπως *ασφάλεια* (security), *ταυτοποίηση* (identification) και *αυθεντικοποίηση* (authentication). Μερικές φορές οδηγεί σε συγκρούσεις και αποτελεί μονόδρομος η εύρεση ισορροπιών. Τα προβλήματα ιδιωτικότητας επιδεινώνονται ραγδαία καθώς οι εφαρμογές «νέφους» αποτελούν μέρος της καθημερινότητας των χρηστών του Διαδικτύου και όχι απλά μια μελλοντική τεχνολογική εξέλιξη.

Στα πλαίσια της παρούσας διπλωματικής εργασίας θα δώσουμε μια τελευταία εικόνα των εξελίξεων των εφαρμογών του *υπολογιστικού νέφους* (cloud computing) με έμφαση στις δυνητικές επιπτώσεις στην ιδιωτικότητα. Το «νέφος» αφορά στην παροχή υπολογιστικών πόρων *κατά ζήτηση* (on demand) μέσω του Διαδικτύου από εταιρείες παρόχους τέτοιων υπηρεσιών. Η πρόσβαση σε υπολογιστικούς πόρους γίνεται από οπουδήποτε αρκεί να υπάρχει σύνδεση στο Διαδίκτυο. Τα πλεονεκτήματα για εταιρείες και επιχειρήσεις είναι πολλά καθώς μειώνονται τα λειτουργικά τους έξοδα. Παρόλα αυτά εκκρεμεί η επίλυση ζητημάτων που αφορούν την έλλειψη προτύπων αγοράς, την ασφάλεια και την ιδιωτικότητα των χρηστών υπηρεσιών «νέφους». Σύμφωνα με πρόσφατη έρευνα σε στελέχη πληροφορικής προκύπτει πως το «νέφος» θα αποτελέσει τον σημαντικότερο μοχλό αύξησης των εσόδων στον συγκεκριμένο τομέα τα επόμενα 3 χρόνια.

Το θέμα των *ηλεκτρονικών ταυτοτήτων* (electronic identity card) αποκτά ιδιαίτερη σημασία στο επερχόμενο πλαίσιο σχετικά πάντοτε με την ιδιωτικότητα. Στην συνέχεια της εργασίας θα παρουσιάσουμε ορισμένες πρόσφατες εξελίξεις στις ηλεκτρονικές ταυτότητες. Οι νέου τύπου ηλεκτρονικές ταυτότητες δεν αποτελούν απλά προϊόν ψηφιοποίησης των συμβατικών ταυτοτήτων, αλλά μία πιο «έξυπνη» μορφή τους. Ενσωματώνουν δυνατότητες για online ταυτοποίηση αλλά και για υπογραφή ηλεκτρονικών εγγράφων μέσω ψηφιακών υπογραφών. Με την διάδοσή τους επαναπροσδιορίζεται το ζήτημα της προστασίας των προσωπικών δεδομένων. Προκύπτει λοιπόν πως τα κλασσικά διαπιστευτήρια που χρησιμοποιούνται συνήθως για να πιστοποιήσει κάποιος χρήστης την ταυτότητά του κατά την διάρκεια των ηλεκτρονικών του συναλλαγών, δεν προστατεύουν πλήρως την ιδιωτικότητα του. Κατά κανόνα αποκαλύπτεται η ταυτότητα του κατόχου του διαπιστευτηρίου, παρόλο που συχνά απαιτείται λιγότερη πληροφορία. Για παράδειγμα, για να ενοικιάσει κανείς ένα αυτοκίνητο αρκεί η επιβεβαίωση πως είναι ενήλικας και δεν είναι απαραίτητο να γίνει γνωστή η ακριβής ημερομηνία γέννησής του. Αντιθέτως, τα διαπιστευτήρια που βασίζονται σε χαρακτηριστικά (Attribute Based Credentials) επιτρέπουν στον κάτοχο του διαπιστευτηρίου να αποκαλύψει μόνο την ελάχιστη πληροφορία που απαιτείται, χωρίς να αποκαλύπτει την πλήρη ταυτότητά του. Αυτό ονομάζεται *ελάχιστη αποκάλυψη* (minimal disclosure).

Λέξεις κλειδιά: υπολογιστικό νέφος, ηλεκτρονικές ταυτότητες, ιδιωτικότητα

Abstract

Privacy is a word we hear quite often nowadays. However it is not easy to give a strict definition. Generally, it is the concern of a person or group of individuals to protect information about them and those they want or those imposed by society or the state, and thus 'revealed' selective. The boundaries and content of what is considered private differs between cultures, countries and different people, but shares basic common themes. As regards the field of Informatics, privacy of information or privacy of data is the correlation between the collection and dissemination of data, technology, society's expectations of privacy and legal issues surrounding all.

The privacy is central to the Web. It intersects issues such as security, identification and authentication. Sometimes it leads to conflict and is one way to find balance. The privacy issues are rapidly deteriorating as the applications of "cloud" becoming part of everyday Internet users and not just a future technology development.

As part of this thesis will give an overview of recent developments in applications of cloud computing, with emphasis on the potential impact on privacy. The "cloud" refers to the provision of computing resources on demand over the Internet from companies providing such services. To have access to computing resources from anywhere is enough to have an Internet connection. The advantages for companies and businesses are many as they reduce their operating costs. Nevertheless, is pending the resolution of issues relating to lack of market standards, security and user's privacy of "cloud" services. According to a recent survey the "cloud" will be the main driver of revenue growth in the Informatics over the next 3 years.

The issue of electronic identity cards is of particular importance in the upcoming framework of privacy. In continuing, the work will present some recent developments in electronic identity cards. The new type of electronic identity cards is not just digitize conventional identities, but are a more intuitive form. Integrate opportunities for online identification and signature for electronic documents through digital signatures. With the proliferation redefined the issue of protection of personal data. The classical credentials which are typically used to certify a user's identity during an

electronic transaction are not fully protect their privacy. Normally reveal the identity of the holder of credentials, although frequently less information is needed. For example, for someone to rent a car is sufficient to confirm that it is an adult and is not necessary to know the exact date of birth. However, the *attribute based credentials* allow the holder of credentials to disclose only the minimum information required (*minimal disclosure*), without disclosing their full identity.

Keywords: cloud computing, electronic id, privacy

Περιεχόμενα

1 Εισαγωγή

Η έννοια της *ιδιωτικότητας* (privacy) σε σχέση με την αυξανόμενη ενσωμάτωση των ψηφιακών τεχνολογιών στην ζωή μας είναι αναμφισβήτητα στην επικαιρότητα. Τα όρια και το περιεχόμενο του τι θεωρείται ιδιωτικό διαφέρει μεταξύ πολιτισμών, ατόμων, ηλικιών και λαών ενώ αλλάζει με το πέρασμα του χρόνου αλλά μοιράζεται ορισμένες βασικές αρχές. Έχει αμφίπλευρη σχέση με την *ασφάλεια* (security) καθώς μερικές φορές οι δύο έννοιες συμβαδίζουν ενώ άλλες συγκρούονται.

Στον χώρο της Πληροφορικής *Ιδιωτικότητα της Πληροφορίας* (information privacy) ή *Ιδιωτικότητα των Δεδομένων* (data privacy) είναι η συσχέτιση ανάμεσα στην συλλογή και διάδοση των δεδομένων, στην τεχνολογία, στην προσδοκία της κοινωνίας για ιδιωτικότητα και στα νομικά ζητήματα που περιβάλλουν όλα αυτά. Τα τελευταία χρόνια με την ευρεία διάδοση του Παγκόσμιου Ιστού και των εφαρμογών του η προστασία της ιδιωτικότητας δημιουργεί διαρκώς νέες προκλήσεις. Η δυνατότητα να ελέγχει κάποιος ποιές πληροφορίες αποκαλύπτονται για τον ίδιον μέσω του Διαδικτύου, και ποιος μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, αποτελεί ένα ζήτημα αυξανόμενης ανησυχίας. Στα προσωπικά δεδομένα ανήκει κάθε δεδομένο που μπορεί πιθανώς να χρησιμοποιηθεί αυτόνομο ή σε συνδυασμό με άλλες πηγές για να ταυτοποιήσει μοναδικά, να σχετίσει ή να εντοπίσει ένα μόνο άτομο.

Παράδειγμα σημαντικής απειλής της ιδιωτικότητας αποτελούν τα κοινωνικά δίκτυα, τα οποία τα τελευταία χρόνια γνωρίζουν μεγάλη ανάπτυξη. Μια από τις πιο γνωστές σελίδες κοινωνικής δικτύωσης είναι και το Facebook. Σύμφωνα με στοιχεία που παρουσίασε η ελληνική μη κυβερνητική οργάνωση N.E.O.I., κατά το 2010 δέχτηκε 218 καταγγελίες, εκ των οποίων το 72% αφορούσε παραβιάσεις προσωπικών δεδομένων στο Facebook, το 16% πορνογραφικά μηνύματα στο ηλεκτρονικό ταχυδρομείο των χρηστών του διαδικτύου, το 2% σεξουαλική παρενόχληση σε προσωπικό ιστολόγιο ή ιστοσελίδα, ενώ έγιναν 6 αναφορές γονέων για εθισμό των παιδιών τους με ηλεκτρονικά παιχνίδια και αυξημένη χρήση του διαδικτύου και άλλες που αφορούσαν οικονομικές απάτες.[1] Ενδεικτικό της έκτασης και της σοβαρότητας της κατάστασης είναι το γεγονός πως η επίτροπος της Ευρωπαϊκής Ένωσης για θέματα δικαιοσύνης προειδοποίησε εταιρείες όπως το Facebook ότι «*μία εταιρεία*

κοινωνικής δικτύωσης που εδρεύει στις ΗΠΑ η οποία έχει εκατομμύρια ενεργών χρηστών στην Ευρώπη πρέπει να συμμορφώνεται με τους κανόνες της Ε.Ε.». Το συνολικό «πακέτο» των προτάσεων θα ανακοινωθεί το καλοκαίρι. Η επίτροπος δήλωσε πως σκοπεύει να αναγκάσει το Facebook και τα άλλα παρεμφερή sites να καθιερώσουν υψηλά στάνταρ προστασίας προσωπικών δεδομένων και να δώσουν στο χρήστη πλήρη έλεγχο σχετικά με το υλικό που διατίθεται online.[2]

Πέραν όμως των κοινωνικών δικτύων υπάρχουν και άλλες εφαρμογές του Διαδικτύου που πιθανώς να μην εξασφαλίζουν στον μέγιστο βαθμό την προστασία της ιδιωτικότητας των χρηστών. Μια από αυτές είναι και το επερχόμενο *Υπολογιστικό Νέφος* ή *Νέφος* (cloud computing) το οποίο πλέον είναι μέρος της καθημερινότητας πολλών μεμονωμένων χρηστών αλλά και επιχειρήσεων. Το «νέφος» αφορά στην παροχή υπολογιστικών πόρων όπως εφαρμογές, βάσεις δεδομένων, υπηρεσίες αρχείων, αποθηκευτικού χώρου, υπολογιστικής ισχύος, e-mail κ.α., *κατ' αίτηση* (on demand) μέσω του Διαδικτύου. Ο ρόλος του υπολογιστή του χρήστη μοιάζει πολύ με εκείνον ενός τερματικού σ' ένα απομακρυσμένο δίκτυο καθώς δεν χρειάζεται να περιέχει δεδομένα ή εφαρμογές, τα οποία και βρίσκονται αποθηκευμένα σε κέντρα δεδομένων κάπου στο Διαδίκτυο χωρίς ο χρήστης να γνωρίζει πού (γι' αυτό συνηθίζεται όταν αναφερόμαστε σε παρεχόμενες υπηρεσίες cloud computing να χρησιμοποιούμε τον όρο «νέφος»). Τα πλεονεκτήματα είναι αρκετά. Οι χρήστες χρησιμοποιούν υπηρεσίες που παρέχονται από παρόχους υπηρεσιών όπως οι εταιρείες Google και Amazon και πληρώνουν για όσο χρησιμοποιούν αυτές τις υπηρεσίες. Επιπλέον μπορούν να αυξήσουν ή να μειώσουν το επίπεδο χρήσης των υπολογιστικών πόρων και των υπηρεσιών ευέλικτα και εύκολα χωρίς να χρειάζεται να γνωρίζουν ή να πρέπει να διαχειριστούν την υποκείμενη τεχνολογία. Η διαχείριση γίνεται από τους παρόχους ενώ το μόνο που χρειάζεται να διαθέτουν οι χρήστες είναι πρόσβαση στο Διαδίκτυο.

Ένα από τα σημαντικότερα προβλήματα που θέτει το «νέφος» είναι η ιδιωτικότητα των πληροφοριών. Τα δεδομένα των χρηστών βρίσκονται κάπου στο «νέφος». Θα πρέπει λοιπόν να εξασφαλιστεί πως τα δεδομένα αυτά δεν θα είναι προσβάσιμα από μη εξουσιοδοτημένους χρήστες. Επιπλέον, η μετάβαση σε συγκεντρωτικές υπηρεσίες θα μπορούσε να επηρεάσει την ιδιωτικότητα και την ασφάλεια στις αλληλεπιδράσεις μεταξύ των χρηστών. Απειλές για την ασφάλεια μπορεί να εμφανιστούν κατά την

διάρκεια εκτέλεσης κατανεμημένων εφαρμογών. Επιπρόσθετα, είναι πιθανό να προκύψουν και νέες απειλές. Ταυτόχρονα θα πρέπει να ενισχυθεί η διαλειτουργικότητα ανάμεσα στους διάφορους παρόχους υπηρεσιών. Ζητούμενο, έστω ουτοπικά, θα ήταν πως η ευρύτερη διάδοση του «νέφους» θα πραγματοποιηθεί μόνο όταν οι χρήστες νοιώσουν σίγουροι πως η ιδιωτικότητα των δεδομένων τους προστατεύεται επαρκώς. Η ανάπτυξη του «νέφους» παρατίθενται σε επόμενο κεφάλαιο.

Σημαντικό όπλο για την ασφάλεια των ηλεκτρονικών συναλλαγών γενικότερα, και των υπηρεσιών «νέφους» ειδικότερα αποτελεί η *αυθεντικοποίηση* (authentication). Ανάμεσα στις διαφορετικές προσεγγίσεις που προτείνονται για επίτευξη της αυθεντικοποίησης είναι και οι ηλεκτρονικές ταυτότητες. Οι ηλεκτρονικές ταυτότητες δεν είναι απλά αποτέλεσμα ψηφιοποίησης των συμβατικών ταυτοτήτων. Προσφέρουν πολύ περισσότερες δυνατότητες όπως online ταυτοποίηση αλλά και υπογραφή ηλεκτρονικών εγγράφων μέσω ψηφιακών υπογραφών. Υπάρχουν ήδη χώρες όπως η Ιταλία και η Γερμανία που έχουν θεσπίσει τις ηλεκτρονικές ταυτότητες ενώ αρκετές διατίθενται να τις υιοθετήσουν στο άμεσο μέλλον.

Γενικά, οι παραδοσιακές ηλεκτρονικές ταυτότητες χρησιμοποιούν κάποιου είδους κλασσικό διαπιστευτήριο, όπως το X.509 ή ηλεκτρονικά πιστοποιητικά, τα οποία όμως δεν προστατεύουν την ιδιωτικότητα του χρήστη. Αυτό συμβαίνει διότι εκθέτουν την ταυτότητα του κατόχου στο μέρος που ζητά την αυθεντικοποίηση. Υπάρχουν πολλά σενάρια όπου η χρήση τέτοιων πιστοποιητικών αποκαλύπτει όλα τα στοιχεία της ταυτότητας του κατόχου χωρίς να είναι απαραίτητο. Π.χ. υπάρχουν σενάρια όπου η παροχή μιας υπηρεσίας χρειάζεται μόνο να εξακριβώσει την ηλικία ενός χρήστη και όχι την πραγματική του/της ταυτότητα. Η αποκάλυψη περισσότερων πληροφοριών από τις απαραίτητες όχι μόνο προσβάλλει δυνητικά την ιδιωτικότητα των χρηστών αλλά αυξάνει και το ρίσκο κακής χρήσης των πληροφοριών του, όπως κλοπή ταυτότητας, όταν οι πληροφορίες πέσουν σε λάθος χέρια. Τα *διαπιστευτήρια που βασίζονται στα χαρακτηριστικά* (Attribute Based Credentials-ABCs) επιτρέπουν στον κάτοχό τους να αποκαλύπτει την ελάχιστη πληροφορία που απαιτείται κατά την διάρκεια μιας συναλλαγής χωρίς να αποκαλύπτεται πλήρως η ταυτότητα του. Ο χρήστης λοιπόν μπορεί να αποδείξει σ' ένα "τρίτο μέρος" ότι έχει στην κατοχή του ένα διαπιστευτήριο που περιέχει ένα συγκεκριμένο χαρακτηριστικό ή ρόλο χωρίς να αποκαλύπτει άλλες πληροφορίες που είναι αποθηκευμένες σε αυτό. Τα ABCs

υπόσχονται να είναι ένας ακρογωνιαίος λίθος για την προστασία της ιδιωτικότητας του χρήστη σ' ένα ηλεκτρονικό περιβάλλον. Περισσότερες πληροφορίες για τις ηλεκτρονικές ταυτότητες και τα ABCs παρατίθενται σε επόμενο κεφάλαιο.

Στο δεύτερο κεφάλαιο της εργασίας γίνεται αναφορά στην ιδιωτικότητα και τα προσωπικά δεδομένα και περιγράφονται παραδείγματα παραβίασης της ιδιωτικότητας στον ηλεκτρονικό κόσμο. Το τρίτο κεφάλαιο αναφέρεται στο «νέφος». Συγκεκριμένα παρατίθεται ο ορισμός του NIST, γίνεται μια ιστορική αναδρομή και περιγράφονται τρόποι αξιοποίησης των δυνατοτήτων του «νέφους» στην εκπαίδευση. Επιπρόσθετα αναφέρονται παραδείγματα παρόχων υπηρεσιών και περιγράφονται οι υπηρεσίες Google Apps και Pithos καθώς και το νέο laptop Chromebook. Επιπλέον αναλύονται πιθανά οφέλη που προσφέρει το «νέφος» αλλά και θέματα που επιζητούν επίλυση. Στο τέταρτο κεφάλαιο περιγράφεται αναλυτικά το έργο ABC4Trust, οι στόχοι του έργου και η συμβολή του στο state of the art. Το επόμενο κεφάλαιο είναι αφιερωμένο στις ηλεκτρονικές ταυτότητες. Συγκεκριμένα παρατίθενται οι νόμοι της ταυτότητας και περιγράφονται εν συντομία η ιταλική και η γερμανική ηλεκτρονική ταυτότητα. Περιγράφονται επίσης 4 πιθανά σενάρια, που για να υλοποιηθούν απαιτείται η ανάπτυξη κατάλληλων υπηρεσιών ψηφιακών ταυτοτήτων σε συνδυασμό με πλήρη αξιοποίηση των δυνατοτήτων που προσφέρει το «νέφος». Στο τελευταίο κεφάλαιο αναφέρονται συμπεράσματα και προοπτικές που προέκυψαν στα πλαίσια της εργασίας.

2 Ιδιωτικότητα

2.1 Τι είναι ιδιωτικότητα;

Δεν είναι εύκολο να δώσει κανείς μονοσήμαντα τον ορισμό του τι είναι *ιδιωτικότητα* (privacy) και είναι αυτό ένα θέμα με κοινωνιολογική και όχι μόνο τεχνολογική διάσταση. Γενικά, είναι η μέριμνα ενός ατόμου ή μιας ομάδας ατόμων να προστατεύουν όσες πληροφορίες σχετικές με αυτούς θέλουν ή όσες επιβάλλονται από την κοινωνία ή/και την πολιτεία και να «αποκαλύπτονται» επιλεκτικά. Τα όρια και το περιεχόμενο του τι θεωρείται ιδιωτικό διαφέρει μεταξύ πολιτισμών, ατόμων, ηλικιών και εποχών, αλλά μοιράζεται βασικά κοινά θέματα. Η ιδιωτικότητα έχει στενή σχέση με την *ασφάλεια* (security), περιλαμβάνει τις έννοιες της «κατάλληλης» χρήσης και προστασίας των πληροφοριών και ενώ συχνά συμπίπτει με την ασφάλεια, άλλες φορές συγκρούεται.

2.2 Προσωπικά δεδομένα

Στα δεδομένα προσωπικού χαρακτήρα (μερικές φορές ονομάζονται και *προσωπικά στοιχεία*) περιλαμβάνεται κάθε δεδομένο που μπορεί πιθανώς να χρησιμοποιηθεί αυτόνομο ή σε συνδυασμό με άλλες πηγές, για να ταυτοποιήσει μοναδικά, να σχετίσει ή να εντοπίσει ένα μόνο πρόσωπο. Παραδείγματα προσωπικών δεδομένων είναι:

- Πληροφορίες επικοινωνίας (όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, τηλέφωνο, ταχυδρομική διεύθυνση)
- Μορφές ταυτοποίησης (ταυτότητα, δίπλωμα οδήγησης, διαβατήριο, δαχτυλικά αποτυπώματα)
- Δημογραφικές πληροφορίες (ηλικία, φύλο, εθνικότητα, θρησκευτικές πεποιθήσεις, σεξουαλικές προτιμήσεις, ποινικό μητρώο)
- Επαγγελματικές πληροφορίες (θέση, όνομα εταιρείας)
- Πληροφορίες υγειονομικής περίθαλψης (κατάσταση υγείας, πάροχοι, ασφάλιση, γενετικές πληροφορίες)

- Χρηματοοικονομικές πληροφορίες (τραπεζικούς και πιστωτικούς/ χρεωστικούς αριθμούς λογαριασμών, ιστορικό αγορών)
- Online δραστηριότητα (διεύθυνση IP, αγορές, επαφές, επισκέψεις, ηλεκτρονικοί φίλοι…)

Ένα υποσύνολο των προσωπικών δεδομένων ορίζεται ως *ευαίσθητα προσωπικά δεδομένα* και απαιτεί ένα μεγαλύτερο επίπεδο ελέγχου όσο αφορά την συλλογή, χρήση, γνωστοποίηση και προστασία. Παραδείγματα πληροφοριών που αποτελούν ευαίσθητα προσωπικά δεδομένα είναι: 1) θρησκευτικές πεποιθήσεις 2) πολιτικές ιδέες και 3) πληροφορίες που αφορούν την υγεία. Τα ευαίσθητα προσωπικά δεδομένα περιλαμβάνουν και κάποιες μορφές ταυτοποίησης, όπως ο αριθμός κοινωνικής ασφάλισης, ορισμένα δημογραφικά δεδομένα, και πληροφορίες που μπορούν να χρησιμοποιηθούν για να αποκτήσει κάποιος πρόσβαση σε χρηματοοικονομικούς λογαριασμούς, όπως αριθμοί πιστωτικών καρτών και αριθμοί λογαριασμών σε συνδυασμό με οποιονδήποτε απαιτούμενο κωδικό ασφαλείας ή κωδικό πρόσβασης.

2.3 Ιδιωτικότητα και νομοθεσία

Από μια πιο νομική σκοπιά, *«η ιδιωτικότητα είναι σημείο ρήξης ανάμεσα στην ελευθερία και την ασφάλεια, λόγω της ανασφάλειας που καλλιεργείται με αφορμή την τρομοκρατία και την εγκληματικότητα, ωθώντας σε μέτρα που συρρικνώνουν τα ατομικά δικαιώματα γενικά και την ιδιωτικότητα ειδικότερα»*. [3]

Στην Ελλάδα, η νομοθεσία διαχωρίζει τις πληροφορίες που αφορούν καθένα από εμάς σε προσωπικά δεδομένα και σε ευαίσθητα προσωπικά δεδομένα με τα δεύτερα να προστατεύονται με ποιον αυστηρό τρόπο από τον νόμο. Αξίζει να αναφερθεί πως το 2007 η χώρα μας κέρδισε μια πρωτιά που δεν πήρε τη δημοσιότητα που της αξίζει: στη «Διεθνή Κατάταξη Ιδιωτικότητας για το 2007» (καταρτίζεται κάθε χρόνο από το αμερικανικό Electronic Privacy Information Center και το αγγλικό Privacy International, βλ. http://www.privacyinternational.org. και «Ελευθεροτυπία» στις 2.1.2008) η Ελλάδα είναι πρώτη στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων ανάμεσα στις 27 χώρες της ΕΕ και σε άλλες 20 χώρες. [4]

Πολλές χώρες έχουν θεσπίσει νόμους για την προστασία της ιδιωτικότητας των ατόμων, όπως ο Personal Information Protection and Electronic Documents Act

(PIPEDA) στον Καναδά, η οδηγία της Ευρωπαϊκής Επιτροπής σχετικά με το απόρρητο των δεδομένων και ο Swiss Federal Data Protection Ordinance. Στις Ηνωμένες Πολιτείες Αμερικής το δικαίωμα των ατόμων για ιδιωτικότητα προστατεύεται και από ρυθμιστικές αξιώσεις που αφορούν τον επιχειρηματικό τομέα όπως η Health Insurance Portability and Accountability Act (HIPAA), η The Gramm-Leach- Bliley Act (GLBA), και η FCC Customer Proprietary Network Information (CPNI).

2.4 Ιδιωτικότητα και Πληροφορική

Όσο αφορά τον χώρο της Πληροφορικής, *Ιδιωτικότητα της πληροφορίας* (information privacy) ή *Ιδιωτικότητα των δεδομένων* (data privacy) είναι η συσχέτιση ανάμεσα στην συλλογή και διάδοση των δεδομένων, στην τεχνολογία, στην προσδοκία της κοινωνίας για ιδιωτικότητα και στα νομικά ζητήματα που περιβάλλουν όλα αυτά. [5] Η δυνατότητα να ελέγχει κάποιος ποιές πληροφορίες αποκαλύπτονται για τον ίδιον μέσω του Διαδικτύου, και ποιος μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, αποτελεί ένα ζήτημα αυξανόμενης ανησυχίας. Τα πεδία της ασφάλειας δεδομένων και της ασφάλειας πληροφοριών σχεδιάζουν και χρησιμοποιούν υλικό, λογισμικό και ανθρώπινους πόρους για να αντιμετωπίσουν αυτό το ζήτημα. Σε επόμενη ενότητα αναφέρονται περισσότερα για την ιδιωτικότητα των χρηστών σ' ένα από τα μεγαλύτερα κοινωνικά δίκτυα, το Facebook.

Η προστασία της ιδιωτικότητας αποτελεί σημαντικό ζήτημα και για τις επιχειρήσεις. Επικεντρώνεται στην διασφάλιση ότι τα προσωπικά δεδομένα των χρηστών προστατεύονται από μη εξουσιοδοτημένη και ανάρμοστη συλλογή, χρήση και αποκάλυψή τους, και σε τελική ανάλυση στην διαφύλαξη της εμπιστοσύνης των πελατών και την παρεμπόδιση δόλιας δραστηριότητας, όπως κλοπή ταυτότητας και ηλεκτρονικό «ψάρεμα» (phishing)[1].

Οι πληροφορίες των πελατών μπορεί να είναι «δεδομένα χρήστη» ή/και «προσωπικά δεδομένα». Τα δεδομένα χρήστη είναι πληροφορίες που συλλέγονται από τον πελάτη και συμπεριλαμβάνουν:

[1] Ηλεκτρονικό «ψάρεμα» είναι η διαδικασία κατά την οποία κάποιος προσπαθεί να αποκτήσει ευαίσθητες πληροφορίες όπως usernames, passwords, ή στοιχεία για πιστωτικές κάρτες, έχοντας την συμπεριφορά ενός αξιόπιστου προσώπου, στα πλαίσια μιας ηλεκτρονικής επικοινωνίας.

- Δεδομένα που συλλέγονται απευθείας από κάποιον πελάτη (π.χ. συμπληρώνονται από τον πελάτη μέσω της διαπεφής μιας εφαρμογής)
- Δεδομένα σχετικά με κάποιον πελάτη που συγκεντρώνονται έμμεσα (π.χ. μεταδεδομένα σε έγγραφα)
- Δεδομένα σχετικά με την συμπεριφορά χρήσης του πελάτη
- Δεδομένα που σχετίζονται με το σύστημα του πελάτη (π.χ διεύθυνση IP)

Να σημειωθεί πως τα δεδομένα χρήστη μπορεί να είναι και προσωπικά δεδομένα.

2.5 Παραδείγματα παραβίασης της ιδιωτικότητας

Παράδειγμα σημαντικής απειλής της ιδιωτικότητας αποτελούν τα κοινωνικά δίκτυα, τα οποία τα τελευταία χρόνια γνωρίζουν μεγάλη διάδοση. Μια από τις πιο γνωστές σελίδες κοινωνικής δικτύωσης είναι και το Facebook. Στην Γερμανία το Facebook κατηγορείται ότι παραβιάζει τη γερμανική νομοθεσία για την ιδιωτικότητα επειδή συλλέγει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου ανθρώπων οι οποίοι δεν διαθέτουν λογαριασμούς στη δημοφιλή υπηρεσία κοινωνικής δικτύωσης. Το λογισμικό του Facebook έχει την δυνατότητα να ψάξει τους υπολογιστές των χρηστών του για να εντοπίζει και να αποθηκεύει τη λίστα επαφών και να υφαρπάζει τα ονόματα και τα e-mail τους. Ο επίτροπος προστασίας της ιδιωτικής ζωής στο Αμβούργο, δήλωσε *«Θεωρούμε ότι η καταγραφή των δεδομένων τρίτων προσώπων είναι ανεπίτρεπτη βάσει των νόμων περί της προστασίας δεδομένων. Θέλουμε να αποδείξουμε ότι η γερμανική νομοθεσία για την προστασία των δεδομένων ισχύει και για τις ξένες εταιρείες που έχουν χρήστες στη Γερμανία»*.[6]

Μια γνωστή εταιρεία που επανειλημμένως έχει δεχθεί καταγγελίες για παραβιάσεις της ιδιωτικότητας των χρηστών είναι η Google. Πρόσφατα η Γαλλία μήνυσε την Google με το ποσό των €100,000 για την συλλογή δεδομένων από ιδιωτικά Wi-Fi δίκτυα κατά την διάρκεια συγκέντρωσης εικόνων για την Google Street View. Η Google Street View είναι μια υπηρεσία των Google Maps και Google Earth που προσφέρει πανοραμική θέα από διάφορες θέσεις κατά μήκος πολλών δρόμων ανά τον κόσμο. Ξεκίνησε στις 25 Μαΐου του 2007, αρχικά μόνο σε κάποιες πόλεις στις Ηνωμένες Πολιτείες, και έκτοτε βαθμιαία επεκτάθηκε ώστε να περιλαμβάνει περισσότερες πόλεις και αγροτικές περιοχές απ’ όλο τον κόσμο. Η Google Street

View εμφανίζει εικόνες που λαμβάνονται από ειδικά εξοπλισμένα αυτοκίνητα. Σε κάθε ένα από αυτά τα αυτοκίνητα υπάρχουν 9 ειδικές κάμερες, GPS και 3G/GSM/Wi-Fi κεραίες για την ανίχνευση 3G/GSM και Wi-Fi hotspots. Η Google Street View αμφισβητήθηκε από την αρχή της λειτουργίας της. Σε πολλούς δεν άρεσε το γεγονός πως η Google μπορούσε να συγκεντρώνει εικόνες από κτήρια, πινακίδες και πρόσωπα. Η εταιρεία απάντησε αποκρύπτοντας ευαίσθητα κομμάτια των εικόνων. Όμως τον Μάιο του 2010 αποκαλύφθηκε πως τα ειδικά εξοπλισμένα αυτοκίνητα που χρησιμοποιούνται για την υπηρεσία, συνέλλεξαν και αποθήκευσαν δεδομένα από ιδιωτικά κρυπτογραφημένα Wi-Fi δίκτυα. Το γεγονός αποδόθηκε σε λάθος. Τον Αύγουστο του 2010, η γαλλική αστυνομία σταμάτησε ένα από τα αυτοκίνητα της Google Street View ύστερα από εντολή της Εθνικής Επιτροπής για την Πληροφορική και τις Ατομικές Ελευθερίες (National Commission for Computing and Civil Liberties-CNIL) για να επιθεωρήσει το κατά πόσον η Google εξακολουθεί να συλλέγει Wi-Fi δεδομένα. Η CNIL δήλωσε πως η εταιρεία δεσμεύτηκε να διαγράψει τα δεδομένα που είχε συλλέξει, αλλά διαπίστωσε πως δεν απέτρεψε τελικά την χρήση των δεδομένων που συλλέχτηκαν, χωρίς όμως οι χρήστες να το γνωρίζουν. Τον Ιούλιο του 2010 η Google είχε δήλωσε πως τα αυτοκίνητα δεν θα συλλέγουν πλέον καθόλου πληροφορίες, αλλά οι επιπτώσεις από το ατύχημα υπενθυμίζουν πόσο δυσάρεστες μπορεί να γίνουν οι συνέπειες από τον μη σεβασμό της ιδιωτικότητας των χρηστών, ειδικά για εταιρείες του βεληνεκούς της Google. [7]

Ένα από τα πιο πρόσφατα τεχνολογικά επιτεύγματα είναι το iPhone4. Διατέθηκε στην αγορά στις 24 Ιουνίου του 2010. Τον Απρίλιο του 2011 έγινε γνωστό πως η συσκευή κατέγραφε δεδομένα σχετικά με την θέση των χρηστών της χωρίς οι ίδιοι να το γνωρίζουν. Η καταγραφή έγινε μέσω του αρχείου με την ονομασία "consolidated.db", και αφορούσε σημεία ασύρματης πρόσβασης και κεραίες του δικτύου κινητής τηλεφωνίας στην ακτίνα του κατόχου του “έξυπνου” τηλεφώνου (όχι τα ακριβή σημεία όπου βρισκόταν, αφού όπως υποστηρίζει η Apple μπορεί να είναι πολύ μακριά) επί έναν ολόκληρο χρόνο. Μάλιστα τα στοιχεία αυτά χρησιμοποίησαν οι ερευνητές Alasdair Allan και Pete Warden για να αναπαράγουν ζωντανά σε χάρτη τις μετακινήσεις ενός κατόχου iPhone επί ένα χρόνο. Σύμφωνα με την εταιρεία, η καταγραφή ήταν αποτέλεσμα λάθους στο σχεδιασμό του λειτουργικού της συστήματος και επιφυλάχτηκε να το διορθώσει. Πράγματι, μέσα σε μια εβδομάδα διατέθηκε η ενημέρωση 4.3.3 του iOS για iPhone και το iPad 3G (μέσω σύνδεσης στο

iTunes). Η Apple είχε απαντήσει σε ερωτήματα σχετικά με τις υπηρεσίες εντοπισμού θέσεως ενώπιον του αμερικανικού Κογκρέσου. Συγκεκριμένα, είχε δικαιολογήσει την καταγραφή των σημείων ασύρματης πρόσβασης και των κεραιών καθώς την αξιοποιούσε ώστε οι εφαρμογές πλοήγησης να ανταποκρίνονται ταχύτερα στα αιτήματα του χρήστη, σε σχέση με την αναζήτηση δορυφόρων (GPS). Εντούτοις, δεν είχε απαντήσει στο ερώτημα γιατί κατέγραφε την ημερομηνία και την ώρα κατά την οποία «πέρασε» ο κάτοχος του κινητού από κάθε σημείο (εξάλλου, η εμβέλεια των Wi-Fi δεν είναι τόσο μεγάλη). Μετά την ενημέρωση του λειτουργικού με την πρώτη διόρθωση, τα δεδομένα θα καταγράφονται μόνο για επτά ημέρες. Μετά τις διαμαρτυρίες αγανακτισμένων χρηστών, η Apple είχε υποσχεθεί ότι δεν θα επιτρέπεται η λήψη αντιγράφων ασφαλείας του επίμαχου αρχείου με τα δεδομένα θέσης σε ηλεκτρονικό υπολογιστή (που θεωρούνται επιρρεπή σε κακόβουλες επιθέσεις). Μια άλλη διόρθωση είναι η κρυπτογράφηση του αρχείου (και στο iPhone4) και η απενεργοποίηση της καταγραφής των σημάτων στα διαθέσιμα σημεία πρόσβασης όταν οι χρήστες έχουν επιλέξει να απενεργοποιήσουν πλήρως όλες τις υπηρεσίες που χρειάζονται δεδομένα θέσης. Σε κάθε περίπτωση, η εταιρεία υποστηρίζει ότι τα δεδομένα θέσης των χρηστών που επιστρέφουν σε αυτή είναι ανώνυμα. Επίσης, τα δεδομένα θέσης μπορεί να είναι διαθέσιμα σε εταιρείες που παρέχουν τοπικές υπηρεσίες μέσω εφαρμογών για το iPhone4, αν και, για να συμβεί αυτό, απαιτείται η συναίνεση του χρήστη. Το ίδιο ισχύει και για τη διάθεση των στοιχείων θέσης σε διαφημιζόμενους μέσω της πλατφόρμας της Apple, iAd. Πάντως ανησυχίες για το ίδιο θέμα εκφράζονται και για τα κινητά με Android, με την Google να παραδέχεται ότι πράγματι αποθηκεύονται δεδομένα θέσης για σύντομο χρονικό διάστημα από χρήστες που έχουν επιλέξει να χρησιμοποιούν υπηρεσίες GPS. [8]

Η προστασία της ιδιωτικότητας είναι ένα σύνθετο πρόβλημα. Η "λύση" του ή μάλλον η εύρεση σωστής ισορροπίας προϋποθέτει συνδυασμό τεχνολογικών επιτευγμάτων και υιοθέτηση κατάλληλου ρυθμιστικού πλαισίου. Το ρυθμιστικό αυτό πλαίσιο πρέπει να μπορεί να εξελίσσεται δυναμικά αναπροσαρμοζόμενο στις τεχνολογικές εξελίξεις. Καθώς το Διαδίκτυο και η χρήση του ενσωματώνεται όλο και περισσότερο στην καθημερινότητά μας, τα προβλήματα ιδιωτικότητας θα αυξάνονται ποσοτικά αλλά και ποιοτικά, καθώς θα προκύπτουν και νέες είδους απειλές. Στο πλαίσιο αυτό μία από αυτές τις νέες απειλές αποτελεί και το «νέφος» το οποίο θα περιγράψουμε στο επόμενο κεφάλαιο.

3. Υπολογιστικό Νέφος

3.1 Εισαγωγή στο «νέφος»

Το *cloud computing* (*Υπολογιστικό Νέφος* ή *Νέφος* είναι η ελληνική ερμηνεία του όρου), είναι περισσότερο ένα πλαίσιο για ένα διαφορετικό επιχειρηματικό μοντέλο παροχής υπηρεσιών και όχι μια τεχνολογία, το οποίο φαίνεται πως θα μονοπωλήσει το ενδιαφέρον των επιστημόνων που ασχολούνται με την Τεχνολογία Πληροφοριών (Information Technology) τα επόμενα χρόνια. Αποτελεί εξέλιξη της διαδεδομένης πλέον υιοθέτησης της τεχνολογίας *εικονικοποίησης* (virtualization) και του μοντέλου *υπολογισμών ωφέλειας* (utility computing). Η βασική ιδέα πίσω από το «νέφος» είναι ότι ***όλα*** που μπορούν να γίνουν με την χρήση υπολογιστή - είτε σ' έναν προσωπικό υπολογιστή είτε σ' ένα κέντρο δεδομένων (data center)[2] κάποιας εταιρείας, από την αποθήκευση δεδομένων και την επικοινωνία μέσω mail μέχρι συνεργασία σε έγγραφα, μπορούν να μετατοπιστούν στο «νέφος». Ένα από τα χαρακτηριστικά του είναι ότι επιτρέπει στους χρήστες να αλληλεπιδρούν με συστήματα, δεδομένα, και ότι άλλο, μ' έναν τρόπο που "ελαχιστοποιεί την απαραίτητη αλληλεπίδραση με τα υποκείμενα επίπεδα της στοίβας τεχνολογιών" [9]. Σύμφωνα με το Cloud Computing Manifesto [10], τα βασικά χαρακτηριστικά του «νέφους» είναι η δυνατότητα δυναμικής κλιμάκωσης της υπολογιστικής ισχύος μ' έναν αποδοτικό τρόπο και η δυνατότητα του καταναλωτή να έχει το μεγαλύτερο μέρος αυτής της ισχύος χωρίς να χρειάζεται να διαχειριστεί την πολυπλοκότητα της υποκείμενης τεχνολογίας.

Το «νέφος» αποτελεί τεράστια αλλαγή στον τρόπο με τον οποίο παρέχονται οι υπολογιστικοί πόροι, καθώς επιτρέπει την αποθήκευση και την επεξεργασία δεδομένων μέσω του Διαδικτύου όπου και αν είμαστε, ακόμα και την χρήση λειτουργικών συστημάτων και εφαρμογών χωρίς ο χρήστης να χρειάζεται να τα αγοράσει και να τα εγκαταστήσει στον υπολογιστή του, αλλά μπορεί πλέον να χρησιμοποιεί αυτούς τους πόρους ως υπηρεσίες. Η παροχή τέτοιων υπηρεσιών είναι παρόμοια με την παροχή ηλεκτρικού ρεύματος, το οποίο υπάρχει όσο χρειαστούμε όποτε το χρειαστούμε και πληρώνουμε μόνο για όσο καταναλώνουμε. Ο καταναλωτής ασχολείται μόνο με το που βρίσκεται η πρίζα και όχι με το πώς

[2] Κέντρο δεδομένων είναι ένας χώρος που χρησιμοποιείται για να στεγάσει συστήματα ηλεκτρονικών υπολογιστών και συναφή εξαρτήματα, όπως τηλεπικοινωνιακά και αποθηκευτικά συστήματα.

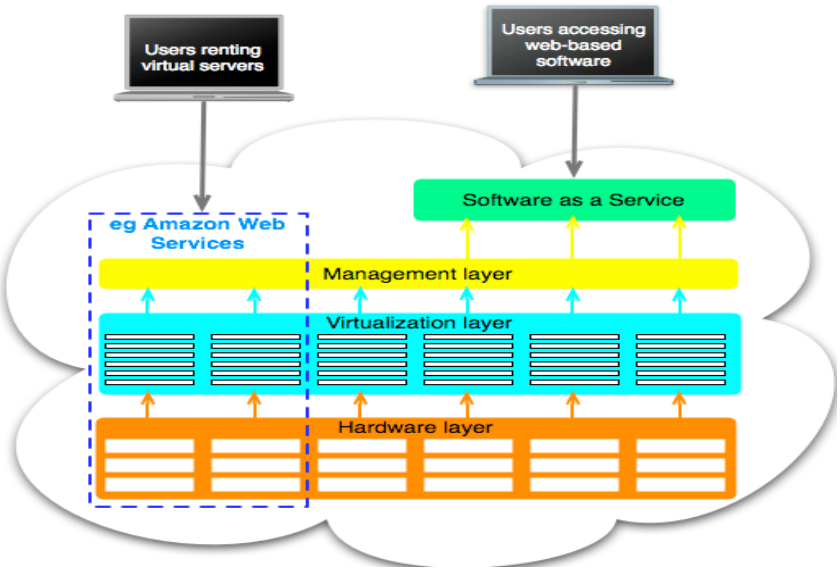
παράγεται ή προσφέρεται η ηλεκτρική ενέργεια. Ήδη υπάρχουν πολλές εταιρείες που προσφέρουν τέτοιες υπηρεσίες και άλλες που το προγραμματίζουν στο άμεσο μέλλον. Παρόλα αυτά υπάρχει σύγχυση σχετικά με το τι είναι οι υπηρεσίες «νέφους», ποια είναι τα οφέλη που προσφέρουν, ποια είναι τα πιθανά μειονεκτήματα και ειδικότερα πόσο ασφαλείς είναι οι υπηρεσίες αυτές και πόσο προστατεύεται η ιδιωτικότητα των χρηστών.

Το «νέφος» είναι συνέπεια της εύκολης πρόσβασης σε απομακρυσμένα site η οποία παρέχεται μέσω του Διαδικτύου. Αυτό συχνά παίρνει την μορφή εργαλείων που βασίζονται στο Web (web-based) ή εφαρμογών, στα οποία οι χρήστες μπορούν να έχουν πρόσβαση και να χρησιμοποιούν μέσα από ένα πρόγραμμα περιήγησης στο web (web browser) σαν να ήταν ένα πρόγραμμα εγκατεστημένο τοπικά στους δικούς τους υπολογιστές. Αντί να διατηρεί ο χρήστης το δικό του περιβάλλον λογισμικού και υλικού, το «νέφος» παρέχει υπολογιστικούς πόρους *κατά ζήτηση* (on demand) μέσω ενός παρόχου υπηρεσιών. Οι υπολογιστικοί πόροι λοιπόν μπορούν να διαμορφώνονται δυναμικά, θεωρητικά χωρίς όρια, ανάλογα με τις απαιτήσεις του χρήστη κάθε χρονική στιγμή. Οι χρήστες πληρώνουν μόνο για τις υπηρεσίες που χρησιμοποιούν και δεν χρειάζεται να γνωρίζουν τίποτα για την τεχνολογία που χρησιμοποιείται, καθώς ο πάροχος είναι εκείνος που διαχειρίζεται την υπηρεσία. Κάποιες φορές ο χρήστης είναι μια συσκευή εξοπλισμένη μ' ένα λειτουργικό σύστημα που «τρέχει» έναν web browser. Δύο είναι τα πιο σημαντικά μέρη της αρχιτεκτονικής του «νέφους»: το κομμάτι που βλέπει ο χρήστης το οποίο περιλαμβάνει το δίκτυο του χρήστη (ή τον υπολογιστή του) και τις εφαρμογές που χρησιμοποιεί για να έχει πρόσβαση στο «νέφος» μέσω ενός περιβάλλοντος διεπαφής, όπως ένας web browser, και το ίδιο το «νέφος» το οποίο περιλαμβάνει ποικίλους υπολογιστές, διακομιστές (servers) και συσκευές αποθήκευσης δεδομένων.

Το «νέφος» έρχεται στον νου όταν σκεφτόμαστε τι χρειάζεται πάντα η Τεχνολογία Πληροφοριών: έναν τρόπο να αυξήσουμε την χωρητικότητα ή να προσθέσουμε δυνατότητες χωρίς να επενδύσουμε σε νέες υποδομές, να εκπαιδεύσουμε προσωπικό ή να αγοράσουμε νέα προγράμματα. Το «νέφος» περικλείει κάθε υπηρεσία την οποία πληρώνουμε *ανάλογα με την χρήση* (pay-per–use), η οποία σε πραγματικό χρόνο μέσω του Διαδικτύου επεκτείνει τις υπάρχουσες δυνατότητες της Τεχνολογίας Πληροφοριών. Σχετίζεται με την ανάγκη κλιμάκωσης των συστημάτων on demand, με το πλεονέκτημα να μπορεί κάποιος να έχει πρόσβαση στα δεδομένα του από

οπουδήποτε χρησιμοποιώντας μια σύνδεση στο Διαδίκτυο, με την δυνατότητα του να αντικαταστήσουμε την συνεχή χρέωση υπηρεσιών με χρέωση ανάλογα με το πόσο χρησιμοποιούμε μια υπηρεσία και τέλος με την επιθυμία των εταιρειών να μειώσουν τα έξοδα που σχετίζονται με την διαχείριση των πόρων υλικού και λογισμικού.

Όσο αφορά την αρχιτεκτονική το κατώτερο επίπεδο είναι το υλικό - οι servers σε κέντρα δεδομένων, είτε ανήκουν σε μια εταιρεία ή κάποιο πανεπιστήμιο για εσωτερική χρήση είτε ανήκουν στην Amazon ή την Google για δημόσια πρόσβαση. Το επόμενο επίπεδο είναι η τεχνολογία εικονικοποιήσης (virtualization), η οποία επιτρέπει σ' έναν server να «τρέχει» πολλούς ανεξάρτητους εικονικούς server. Η αυτοματοποίηση της κατανομής των υπολογιστικών πόρων ανάμεσα στους εικονικούς server και η παρακολούθηση της χρήσης των πόρων από τον χρήστη (πελάτη) απαιτεί ένα επίπεδο διαχείρισης. Αυτό επιτρέπει αληθινή "pay-per-use" χρέωση, κάτι το οποίο ελκύει ιδιαίτερα τους χρήστες του «νέφους». Το επίπεδο διαχείρισης προσφέρει ένα σύνολο υπηρεσιών, που επιτρέπουν στους χρήστες να εκμεταλλεύονται την επεξεργαστική και αποθηκευτική ικανότητα του «νέφους». Αλλά το «νέφος» δεν σταματά εδώ. Η παροχή λογισμικού σε τελικούς χρήστες μέσω του Διαδικτύου είναι αυτό που ονομάζουμε Λογισμικό ως Υπηρεσία (Software as a Service). Αυτό δημιουργεί ένα ακόμα επίπεδο - το λογισμικό «τρέχει» στο «νέφος» και μπορούν οι χρήστες να έχουν πρόσβαση σε αυτό μέσω ενός web browser ή μέσω ενός εργαλείου που είναι συμβατό με το Web.



Εικόνα 1. Ένα απλό μοντέλο επιπέδων του «νέφους»

Σίγουρα το «νέφος» δίνει μια νέα προοπτική στον τρόπο που επικοινωνούμε, συνεργαζόμαστε και λειτουργούμε ανεξαρτήτου πλατφόρμας και φυσικής τοποθεσίας. Έτσι όσο μπορεί κάποιος να έχει πρόσβαση στο Web, μπορεί να εργαστεί όπου και όταν θέλει. Με μια γρήγορη και αξιόπιστη σύνδεση δεν έχει σημασία που βρίσκεται το έγγραφο, το email ή τα δεδομένα που ο χρήστης βλέπει στην οθόνη του. Χτίζοντας πάνω στο Web 2.0, προχωρούμε στην εποχή της "πανταχού υπολογιστικότητας" – με δεδομένα, επικοινωνία και εφαρμογές να βρίσκονται όπου τα χρειαστούμε αρκεί να έχουμε συνδεσιμότητα. Και το Διαδίκτυο σήμερα βρίσκεται παντού γύρω μας. Σημεία ασύρματης πρόσβασης υπάρχουν στα σπίτια μας, στον χώρο δουλειάς, σε δημόσιους χώρους ακόμα και σε εμπορικά καταστήματα [11]. Επίσης έχουμε έναν πλούτο ψηφιακών συσκευών, από υπολογιστές γραφείου και φορητούς υπολογιστές μέχρι συσκευές χειρός, smart phones και netbooks. Κάθε ένα από αυτά έχει ένα πλήθος από δυνατότητες-εφαρμογές για επικοινωνία, και περιεχόμενο. Σήμερα παρόλα, αυτά για πρώτη φορά υπάρχει η προοπτική σύνδεσης αυτών των προηγουμένως ανεξάρτητων συσκευών. Με το «νέφος», "η πληροφορία δεν απομονώνεται σε προσωπικές συσκευές αλλά συνενώνεται σ' ένα ψηφιακό «νέφος» το οποίο είναι διαθέσιμο μ' ένα άγγιγμα του δαχτύλου μας σε πολλές διαφορετικές συσκευές" [12]. Σύμφωνα με το IDC [13], ο αριθμός των συσκευών που έχουν πρόσβαση στο Internet παγκοσμίως, θα αυξηθεί παραπάνω από 3 δισεκατομμύρια μέχρι το 2012 – διπλάσιος αριθμός σε σχέση με το 2008. Μισές από αυτές τις συσκευές θα είναι κινητά, laptops, netbooks, και PDAs. Η IDC προβλέπει πως ο αριθμός των χρηστών που θα έχουν πρόσβαση στο Web μέσω κινητών συσκευών θα τριπλασιαστεί σε σχέση με τον αντίστοιχο αριθμό του 2008 και θα υπερβεί το 1.5 δισεκατομμύριο παγκοσμίως μέχρι το 2012.

3.2 Ο ορισμός του NIST

Στην συνέχεια παραθέτουμε τον ορισμό του National Institute of Standards and Technology (NIST) για το «νέφος» [14]. Ο ορισμός ξεκινά με δύο σημειώσεις:

Σημείωση 1: Το «νέφος» εξελίσσεται διαρκώς. Ορισμοί που σχετίζονται με αυτό, περιπτώσεις χρήσεις, υποκείμενες τεχνολογίες, κίνδυνοι και οφέλη θα τελειοποιηθούν

μέσα από διάλογο με δημόσιους και ιδιωτικούς φορείς. Αυτοί οι ορισμοί και τα χαρακτηριστικά θα αλλάζουν και θα εξελίσσονται με την πάροδο του χρόνου.

Σημείωση 2: Η βιομηχανία του «νέφους» αντιπροσωπεύει ένα μεγάλο σύστημα από πολλά μοντέλα, πωλητές - κατασκευαστές και εξειδικευμένα τμήματα αγοράς. Ο παρών ορισμός προσπαθεί να συμπεριλάβει τις ποικίλες προσεγγίσεις του «νέφους».

Ορισμός: Το «νέφος» είναι ένα μοντέλο που επιτρέπει on-demand πρόσβαση μέσω δικτύου σε μια κοινόχρηστη δεξαμενή[3] διαμορφώσιμων υπολογιστικών πόρων (δίκτυα, servers, μνήμη, εφαρμογές και υπηρεσίες) που μπορούν να προσφερθούν με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο της υπηρεσίας. Αυτό το μοντέλο προωθεί την διαθεσιμότητα, και αποτελείται από πέντε απαραίτητα χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης.

Απαραίτητα χαρακτηριστικά

On-demand self-service: παρέχονται μονομερώς στους καταναλωτές υπολογιστικές δυνατότητες, όπως χρόνος ενός server και δικτυακή αποθήκευση, αυτόματα για όσο τις χρειάζονται χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με τον πάροχο κάθε υπηρεσίας.

Ευρεία δικτυακή πρόσβαση: οι δυνατότητες του «νέφους» είναι διαθέσιμες μέσω δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών που προωθούν την χρήση τους από ετερογενείς πλατφόρμες πελατών (π.χ. κινητά τηλέφωνα, laptops, PDAs).

Διάθεση των πόρων: οι υπολογιστικοί πόροι των παρόχων συγκεντρώνονται για να εξυπηρετήσουν πολλαπλούς πελάτες χρησιμοποιώντας ένα μοντέλο multi-tenant[4], με διαφορετικούς εικονικούς και φυσικούς πόρους να παραχωρούνται δυναμικά ανάλογα με την ζήτηση των καταναλωτών. Υπάρχει μια αίσθηση ανεξαρτησίας όσο αφορά την

[3] Δεξαμενή στην επιστήμη των υπολογιστών είναι ένα σύνολο αρχικοποιημένων πόρων που φυλάσσονται έτοιμοι για χρήση, αντί να κατανέμονται και να καταστρέφονται on demand. Ένας πελάτης θα ζητήσει ένα αντικείμενο και θα εκτελέσει εργασίες στο επιστρεφόμενο αντικείμενο. Όταν ο πελάτης τελειώσει με το αντικείμενο (ή τον πόρο), το επιστρέφει στην δεξαμενή, αντί να τον καταστρέψει.

[4] Αναφέρεται σε μια αρχή στην αρχιτεκτονική λογισμικού σύμφωνα με την οποία ένα λογισμικό εκτελείται στον server, εξυπηρετώντας πολλαπλούς οργανισμούς πελατών (tenants). Με μια multi-tenant αρχιτεκτονική, μια εφαρμογή λογισμικού έχει σχεδιαστεί για να διαχωρίσει εικονικά τα δεδομένα και τις ρυθμίσεις της, και κάθε οργανισμός-πελάτης εργάζεται με ένα προσαρμοσμένο εικονικό στιγμιότυπο της εφαρμογής. Δηλαδή δεν υπάρχει ξεχωριστή εγκατάσταση για κάθε πελάτη. Ουσιαστικά, όλοι οι πελάτες συνυπάρχουν στον ίδιο χώρο και λειτουργούν το ίδιο λογισμικό, αλλά ο καθένας αγνοεί την ύπαρξη του άλλου.

φυσική τοποθεσία, καθώς ο καταναλωτής δεν ελέγχει ή δεν γνωρίζει την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά ίσως να μπορεί να προσδιορίσει την τοποθεσία σ' ένα υψηλότερο επίπεδο αφαίρεσης (π.χ. χώρα, κράτος ή κέντρο δεδομένων). Παραδείγματα παρεχομένων πόρων περιλαμβάνουν επεξεργασία, μνήμη, εύρος δικτύου και εικονικές μηχανές.

Γρήγορη προσαρμοστικότητα: οι δυνατότητες του «νέφους» μπορούν να παρέχονται γρήγορα και με μεγάλη προσαρμοστικότητα, σε κάποιες περιπτώσεις αυτόματα. Στους καταναλωτές οι δυνατότητες που διατίθενται, συχνά φαίνονται να είναι απεριόριστες και μπορούν να τις αγοράσουν σε οποιαδήποτε ποσότητα, οποιαδήποτε χρονική στιγμή.

Μετρούμενη υπηρεσία: τα συστήματα «νέφους» ελέγχουν αυτόματα και βελτιστοποιούν την χρήση των πόρων χρησιμοποιώντας δυνατότητες μέτρησης σε ένα επίπεδο αφαίρεσης κατάλληλο για το τύπο της υπηρεσίας (π.χ. μνήμη, επεξεργασία, εύρος και ενεργοί λογαριασμοί χρηστών). Η χρήση των πόρων μπορεί να παρακολουθηθεί. να ελεγθεί και να καταγραφεί παρέχοντας διαφάνεια για τον καταναλωτή και τον πάροχο της χρησιμοποιούμενης υπηρεσίας.

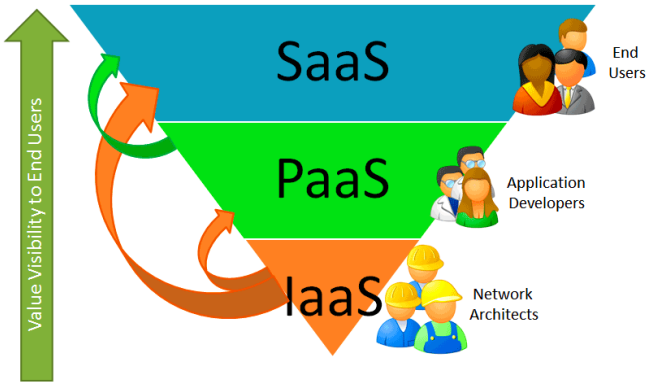
Μοντέλα υπηρεσιών

Λογισμικό ως υπηρεσία (Software as a Service-SaaS): προσφέρεται στον καταναλωτή η δυνατότητα να χρησιμοποιεί τις εφαρμογές του παρόχου που «τρέχουν» σε μια υποδομή του «νέφους». Οι εφαρμογές είναι προσβάσιμες μέσα από τις ποικίλες συσκευές των πελατών, όπως ένας web browser (π.χ. web-based email). Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή, συμπεριλαμβανομένου του δικτύου, των servers, των λειτουργικών συστημάτων και της μνήμης, με πιθανή εξαίρεση τις ρυθμίσεις διαμόρφωσης περιορισμένων εφαρμογών για συγκεκριμένους χρήστες.

Πλατφόρμα ως υπηρεσία (Platform as a Service-PaaS): προσφέρεται στον καταναλωτή η δυνατότητα να αναπτύξει πάνω στην υποδομή του «νέφους», εφαρμογές ή αποκτηθείσες εφαρμογές χρησιμοποιώντας γλώσσες προγραμματισμού και εργαλεία που υποστηρίζονται από τον πάροχο. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή, συμπεριλαμβανομένου του δικτύου, των servers,

των λειτουργικών συστημάτων και της μνήμης αλλά έχει τον έλεγχο στις αναπτυσσόμενες εφαρμογές και πιθανώς σε εφαρμογές που φιλοξενούν διαμορφώσεις περιβάλλοντος.

Υποδομή ως υπηρεσία (Infrastructure as a Service-Iaas): προσφέρεται στον καταναλωτή η δυνατότητα να αναπτύξει και να «τρέξει» αυθαίρετο λογισμικό, που μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές, χρησιμοποιώντας βασικούς υπολογιστικούς πόρους όπως επεξεργασία, μνήμη και δίκτυα. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή, αλλά έχει τον έλεγχο σε λειτουργικά συστήματα, μνήμη, αναπτυσσόμενες εφαρμογές, και πιθανώς περιορισμένο έλεγχο σε επιλεγμένα μέρη του δικτύου (π.χ. host firewalls).



Εικόνα 2. Μοντέλα υπηρεσιών του «νέφους»

Μοντέλα ανάπτυξης

Ιδιωτικό «νέφος» (Private cloud): η υποδομή του «νέφους» λειτουργεί αποκλειστικά για έναν οργανισμό. Μπορεί να την διαχειρίζεται ένας οργανισμός ή ένα τρίτο μέρος και μπορεί να υπάρχει εντός χώρου ή εκτός χώρου.

Κοινοτικό «νέφος» (Community cloud): η υποδομή του «νέφους» μοιράζεται σε διάφορους οργανισμούς και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινά ενδιαφέροντα (π.χ. αποστολή, απαιτήσεις ασφάλειας και πολιτική). Μπορεί να την διαχειρίζονται οργανισμοί ή ένα τρίτο πρόσωπο και μπορεί να υπάρχει εντός χώρου ή εκτός χώρου.

Δημόσιο «νέφος» (Public cloud): Η υποδομή του «νέφους» διατίθεται στο ευρύ κοινό ή μια μεγάλη ομάδα της βιομηχανίας και ανήκει σε έναν οργανισμό που πουλά τις υπηρεσίες.

Υβριδικό «νέφος» (Hybrid cloud): η υποδομή του «νέφους» είναι μια σύνθεση δύο ή περισσότερων «νεφών», (ιδιωτικό, κοινοτικό ή δημόσιο) που παραμένουν μοναδικές οντότητες αλλά συνδέονται μεταξύ τους με τυποποιημένη ή ιδιόκτητη τεχνολογία που επιτρέπει φορητότητα σε δεδομένα και εφαρμογές.

3.3 Ιστορική αναδρομή

Η πρωταρχική ιδέα της διανομής υπολογιστικών πόρων μέσω ενός παγκόσμιου δικτύου έχει τις ρίζες της στην δεκαετία του 1960. Σχεδόν όλα τα σύγχρονα χαρακτηριστικά του «νέφους», η σύγκρισή του με την βιομηχανία ηλεκτρικής ενέργειας, και οι διαφορετικές μορφές του είχαν διερευνηθεί στο βιβλίο του Douglas Parkhill's, The Challenge of the Computer Utility το 1966.

Ο όρος «νέφος» προέρχεται από την τηλεφωνία όπου οι τηλεπικοινωνιακές εταιρείες, που μέχρι το 1990 προσέφεραν κυρίως αποκλειστικά point-to-point κυκλώματα, άρχισαν να προσφέρουν υπηρεσίες Εικονικών Ιδιωτικών Δικτύων (Virtual Private Network-VPN)[5] με συγκρίσιμη ποιότητα υπηρεσίας αλλά με χαμηλότερο κόστος. Το σύμβολο του νέφους χρησιμοποιήθηκε για να υποδηλώσει το σημείο οριοθέτησης ανάμεσα σε αυτό που είναι ευθύνη του παρόχου και αυτό που είναι ευθύνη του χρήστη. Το «νέφος» επεκτείνει αυτό το όριο για να καλύψει servers καθώς και υποδομή δικτύου. Η πρώτη επιστημονική χρήση του όρου «*cloud computing*» έγινε σε μια διάλεξη το 1997 από τον Ramnath Chellappa.

Η ιδέα ενός "παγκόσμιου δικτυού υπολογιστών" εμφανίστηκε την δεκαετία του 1960 από τον JCR Licklider, ο οποίος ήταν υπεύθυνος για την ανάπτυξη του ARPANET (Advanced Research Projects Agency Network). Το όραμα του ήταν να μπορούν όλοι στον πλανήτη να διασυνδεθούν και να έχουν πρόσβαση σε προγράμματα και

[5] Ένα εικονικό ιδιωτικό δίκτυο (Virtual Private Network – VPN) είναι ένα δίκτυο υπολογιστών που χρησιμοποιεί την δημόσια υποδομή τηλεπικοινωνιών, όπως κάνει και το Διαδίκτυο, για να παρέχει σε απομακρυσμένες δημόσιες υπηρεσίες ή σε μεμονωμένους χρήστες ασφαλή πρόσβαση στο δίκτυο ενός οργανισμού. Στόχος του είναι να αποφευχθεί ένα ακριβό σύστημα ιδιόκτητων ή μισθωμένων γραμμών που μπορούν να χρησιμοποιηθούν από ένα μόνο οργανισμό.

δεδομένα, σε κάθε δικτυακό τόπο, από οπουδήποτε. Είναι ένα όραμα που μοιάζει πολύ με αυτό που ονομάζουμε «νέφος». Άλλοι ειδικοί αποδίδουν την έννοια του «νέφους» στον John McCarthy ο οποίος πρότεινε την ιδέα η υπολογιστικότητα να μπορεί να διανέμεται σαν υπηρεσία κοινής ωφέλειας.

Από την δεκαετία του 1960, το «νέφος» έχει αναπτυχθεί σε πολλά επίπεδα. Παρόλα αυτά, είχε αργή ανάπτυξη για το κοινό μέχρι την δεκαετία του 1990 που το Διαδίκτυο άρχισε να προσφέρει σημαντικό εύρος ζώνης,.

Ένα από τα πρώτα ορόσημα στην εξέλιξη του «νέφους» ήταν η άφιξη του Salesforce.com το 1999, που πρωτοπόρησε την ιδέα της παροχής εφαρμογών σε επιχειρήσεις μέσω ενός απλού website. Η εταιρεία άνοιξε τον δρόμο σε εξειδικευμένες και μη εταιρείες να παρέχουν εφαρμογές μέσω του Διαδικτύου.

Η Amazon έπαιξε καθοριστικό ρόλο στην εξέλιξη του «νέφους» εκσυγχρονίζοντας τα κέντρα δεδομένων, τα οποία όπως τα περισσότερα δίκτυα υπολογιστών, χρησιμοποιούσαν το 10% της χωρητικότητάς τους κάθε χρονική στιγμή. Αφού διαπιστώθηκε ότι η αρχιτεκτονική του «νέφους» οδήγησε σε σημαντικές βελτιώσεις στην απόδοση, η Amazon ξεκίνησε μια προσπάθεια ανάπτυξης νέων προϊόντων για παροχή υπηρεσιών σε εξωτερικούς πελάτες και εισήγαγε το Amazon Web Service (AWS) το 2006.[15] Στην συνέχεια το 2006, λάνσαρε το Elastic Compute cloud (EC2) ως εμπορική υπηρεσία Ιστού που επέτρεπε σε μικρές επιχειρήσεις και ιδιώτες να νοικιάσουν υπολογιστές για να «τρέχουν» τις δικές τους εφαρμογές.

Το 2007, η Google, η IBM και κάποια πανεπιστήμια ξεκίνησαν ένα ερευνητικό έργο μεγάλης κλίμακας για το «νέφος». [16] Στις αρχές του 2008, το Eucalyptus έγινε η πρώτη AWS API πλατφόρμα ανοιχτού κώδικα για την ανάπτυξη ιδιωτικών «νεφών». Ένα άλλο μεγάλο βήμα έγινε το 2009, καθώς το Web 2.0 έφτασε στο απόγειο του, ενώ η Google και άλλες εταιρείες άρχισαν να προσφέρουν browser-based επιχειρησιακές εφαρμογές, όπως το Google Apps.

Τον Μάρτιο του 2010, ο Steve Ballmer της Microsoft, δήλωσε για το μέλλον της εταιρείας: "Το 75 % των ανθρώπων μας χρησιμοποιούν αποκλειστικά εξ' ολοκλήρου το «νέφος», σ' ένα χρόνο από τώρα το ποσοστό αυτό θα είναι 90 %". [17]

3.4 Ορισμοί

Στην παρούσα ενότητα εξηγούνται όροι που συσχετίζονται με το «νέφος» ώστε να γίνει πιο κατανοητή η έννοια.

Κατά ζήτηση (On-demand): Η βασική προϋπόθεση που θα πρέπει να ικανοποιεί ο πάροχος υπηρεσιών «νέφους» είναι να μπορεί να διανέμει υπολογιστικούς πόρους όταν ο πελάτης τους χρειάζεται. Από την πλευρά του πελάτη, οι διαθέσιμοι υπολογιστικοί πόροι πρέπει είναι σχεδόν άπειροι (π.χ. ο πελάτης δεν περιορίζεται από το σύνολο των server και είναι ευθύνη του παρόχου να έχει αρκετούς πόρους ώστε να ικανοποιήσει τις απαιτήσεις όλων των πελατών). Το να αξιοποιούνται οι υπολογιστικοί πόροι on-demand, είναι μια από τις πιο επιθυμητές δυνατότητες για ένα μεγάλο αριθμό επιχειρήσεων, γιατί εξαλείφει την ανάγκη προγραμματισμού, αγοράς και εγκατάστασης πόρων που θα χρειαστούν κάποια χρονική στιγμή στο μέλλον. Αυτό επιτρέπει στον πελάτη-επιχείρηση να αποφεύγει μια περιττή επένδυση σε πόρους. Επιπλέον, συγκρίνοντας το «νέφος» με το παραδοσιακό μοντέλο του να έχει μια επιχείρηση δικούς της πόρους (π.χ. server), το «νέφος» μειώνει το κόστος που δημιουργείται όταν έχουμε πόρους που δεν χρησιμοποιούνται πλήρως. Συνέπεια αυτού του χαρακτηριστικού των on-demand υπολογιστικών πόρων είναι το γεγονός πως οι προμηθευτές λογισμικού μπορούν να αναπτύξουν εφαρμογές χωρίς να πρέπει εκ των προτέρων να προβλέπουν ένα συγκεκριμένο αριθμό πελατών. [18]

Πληρωμή ανάλογα με την χρήση (Pay-per-use): Είναι μια άλλη πτυχή του «νέφους» που βασίζεται σ' ένα μοντέλο χρέωσης. Ο πελάτης πληρώνει μόνο για βραχυπρόθεσμη χρήση των πόρων και αυτή η χρήση μπορεί να μετρηθεί, για παράδειγμα ανά ώρες ή μέρες, μετατρέποντας αυτό που θα έπρεπε να είναι κεφαλαιακές δαπάνες (capital expenses-CAPEX) σε λειτουργικές δαπάνες (operational expenses-OPEX)[6]. Η έννοια του «νέφους» είναι στενά συνδεδεμένη με την ιδέα του utility computing. Και στις δυο περιπτώσεις, οι υπολογιστικοί πόροι προσφέρονται on-demand, όπως το ηλεκτρικό ρεύμα, το νερό και το φυσικό αέριο

[6] Λειτουργικές δαπάνες είναι ένα συνεχιζόμενο κόστος για την λειτουργία ενός προϊόντος, επιχείρησης ή συστήματος. Κεφαλαιακές δαπάνες, είναι το κόστος της ανάπτυξης ή παροχής μη αναλώσιμων μερών για ένα προϊόν ή σύστημα. Για παράδειγμα, η αγορά ενός φωτοτυπικού αποτελεί κεφαλαιακές δαπάνες, και το κόστος μιας χρονιάς για το χαρτί, μελάνι, ηλεκτρικό ρεύμα και συντήρηση του φωτοτυπικού αποτελούν λειτουργικές δαπάνες.

παρέχονται από μια επιχείρηση κοινής ωφέλειας, αλλά στην περίπτωση των υπολογιστικών πόρων ο καταναλωτής ουσιαστικά τους νοικιάζει. Παρόλα αυτά, σε αντίθεση με μια παραδοσιακή συμφωνία μίσθωσης όπου οι πόροι θα βρίσκονταν στον φυσικό χώρο του πελάτη, στην περίπτωση του «νέφους» οι πόροι βρίσκονται απλά κάπου μέσα στο «νέφος»- και όχι σε μια καθορισμένη φυσική τοποθεσία. Επιπλέον να σημειωθεί ότι σε αντίθεση με την περίπτωση του νερού και του φυσικού αερίου, τα οποία όταν δεν χρησιμοποιούνται είναι διαθέσιμα για μετέπειτα χρήση - το να μην χρησιμοποιείται η επεξεργαστική ισχύς αυτή η ισχύς στην πραγματικότητα σπαταλάτε - αφού δεν θα είναι διαθέσιμη για μετέπειτα χρήση. Επομένως είναι συμφέρον για τον πάροχο των υπηρεσιών «νέφους» να δεχτεί η επιχείρηση-πελάτης να αξιοποιήσει όλη (ή σχεδόν όλη) αυτή την επεξεργαστική ισχύ. [19]

Εικονικοποίηση (Virtualization): Είναι μια μέθοδος για να «τρέχουν» πολλά ανεξάρτητα εικονικά λειτουργικά συστήματα σ' έναν μόνο υπολογιστή. Αυτή η προσέγγιση μεγιστοποιεί το κέρδος από την επένδυση για τον υπολογιστή. Ο όρος επινοήθηκε την δεκαετία του 1690 αναφορικά με την εικονική μηχανή (virtual machine). Η δημιουργία και η διαχείριση εικονικών μηχανών συχνά αποκαλείται πλατφόρμα virtualization (platform virtualization). Η πλατφόρμα virtualization εκτελείται σε ένα συγκεκριμένο υπολογιστή από το λογισμικό που ονομάζεται *πρόγραμμα ελέγχου* (control program). Το πρόγραμμα ελέγχου δημιουργεί ένα περιβάλλον προσομοίωσης, έναν εικονικό υπολογιστή, ο οποίος επιτρέπει στη συσκευή να χρησιμοποιεί ειδικό λογισμικό για το εικονικό περιβάλλον, που συχνά ονομάζεται φιλοξενούμενο λογισμικό (guest software).

Η μέθοδος virtualization σε υπολογιστές ή λειτουργικά συστήματα κρύβει από τους χρήστες τα φυσικά χαρακτηριστικά μιας υπολογιστικής πλατφόρμας, αντί αυτού δείχνει μια αφηρημένη υπολογιστική πλατφόρμα. Ένας «επόπτης» (hypervisor) είναι ένα τμήμα του λογισμικού virtualization που επιτρέπει σε πολλαπλά λειτουργικά συστήματα να εκτελούνται ταυτόχρονα σ' έναν υπολογιστή. Παραδείγματα εταιρειών που παρέχουν τέτοια περιβάλλοντα είναι οι VMware, Microsoft, και Citrix Systems.

Η μέθοδος virtualization αποτελεί μια σταθερή βάση για όλες τις αρχιτεκτονικές «νέφους». Επιτρέπει την γενίκευση και συγκέντρωση των πόρων των κέντρων δεδομένων, δημιουργώντας έτσι έναν πόρο που μπορεί μοιραστεί σε όλες τις εφαρμογές. Με την αποσύνδεση της φυσικής υποδομής από τις εφαρμογές και τις

υπηρεσίες που φιλοξενούνται, η μέθοδος virtualization επιτρέπει μεγαλύτερη αποτελεσματικότητα και ευελιξία, χωρίς καμιά επίπτωση στην παραγωγικότητα του διαχειριστή του συστήματος, ή των εργαλείων και των διαδικασιών. Με τον διαχωρισμό του φόρτου εργασίας από το υποκείμενο λειτουργικό σύστημα και υλικό, η μέθοδος virtualization επιτρέπει μεγάλη μεταφερσιμότητα. Όταν επεκτείνεται σε κάθε στοιχείο του συστήματος π.χ. επιφάνεια εργασίας, δίκτυο, μνήμη και server, επιτρέπει την κινητικότητα των εφαρμογών και των δεδομένων, όχι μόνο σε server και μνήμη αλλά και σε κέντρα δεδομένων και δίκτυα. Παρόλο που πολλοί οργανισμοί στρέφονται στην μέθοδο virtualization για να μειώσουν τις κεφαλαιακές και λειτουργικές δαπάνες τους, ο απώτερος στόχος στο «νέφος» είναι ο διαχωρισμός ανάμεσα σε εφαρμογές και υποδομή. [20]

Υπολογισμοί ωφέλειας (Utility computing): Είναι ο συνδυασμός υπολογιστικών πόρων ως μια μετρούμενη υπηρεσία παρόμοια με τις υπηρεσίας κοινής ωφέλειας (όπως ηλεκτρικό ρεύμα, νερό, φυσικό αέριο και τηλέφωνο). Αυτό το μοντέλο έχει το πλεονέκτημα ότι το αρχικό κόστος για την απόκτηση υπολογιστικών πόρων είναι χαμηλό ή μηδενικό. Αντί αυτού, οι υπολογιστικοί πόροι στην ουσία ενοικιάζονται, μετατρέποντας την ανάγκη για αγορά προϊόντων (υλικό, λογισμικό και εύρος ζώνης δικτύου) σε υπηρεσίες. Ξεκινώντας το 2002 έγινε το θεμέλιο για το μοντέλο του «νέφους το οποίο διέδωσε περεταίρω την ιδέα της χρήσης υπολογιστών, εφαρμογών και δικτύων ως υπηρεσία. Αρχικά υπήρξε κάποιος σκεπτικισμός γι' αυτή την τόσο μεγάλη αλλαγή. Παρόλα αυτά, το νέο αυτό μοντέλο έγινε η κυρίαρχη τάση με την δημοσίευση του βιβλίου "The Big Switch" του Nick Carr. Οι εταιρείες IBM, HP και Microsoft ήταν από τους πρώτους ηγέτες στην περιοχή του utility computing με ερευνητές να εργάζονται στις προκλήσεις αρχιτεκτονικής και ανάπτυξης αυτού του νέου υπολογιστικού μοντέλου. Οι εταιρείες Google, Amazon καθώς και άλλες άρχισαν να έχουν το προβάδισμα το 2008, καθώς καθιέρωσαν τις δικές τους utility υπηρεσίες για εφαρμογές.

Το utility computing εμπεριέχει κάποια μορφή της τεχνολογίας virtualization ώστε η ποσότητα της μνήμης και της υπολογιστικής ισχύος που είναι διαθέσιμη να είναι σημαντικά μεγαλύτερη από αυτή ενός μόνο υπολογιστή με διαμοιρασμό χρόνου (time-sharing). Για να πραγματοποιηθεί αυτό χρησιμοποιούνται στο παρασκήνιο πολλαπλοί servers. Αυτοί μπορεί να είναι μια εξειδικευμένη συστοιχία υπολογιστών που κατασκευάστηκε ειδικά για τον σκοπό της εκμίσθωσης, ή ακόμα και ένας

υποχρησιμοποιούμενος υπερυπολογιστής (supercomputer). Η τεχνική για την εκτέλεση απλών υπολογισμών σε πολλαπλούς υπολογιστές είναι γνωστή ως *Κατανεμημένη Πληροφορική* (Distributed Computing)[7][21]

3.5 «Νέφος» και εκπαίδευση

Οι υπηρεσίες και οι δυνατότητες που προσφέρει το «νέφος» θα μπορούσαν πιθανώς να αξιοποιηθούν στα πλαίσια την εκπαίδευσης. Το «νέφος» μπορεί να συμβάλλει στη διείσδυση και την αξιοποίηση των ΤΠΕ στην εκπαίδευση. Οι εκπαιδευτικοί μπορούν να χρησιμοποιήσουν μεγάλο πλήθος εκπαιδευτικών λογισμικών, τα οποία είναι ανά πάσα στιγμή διαθέσιμα από οποιοδήποτε Η/Υ με πρόσβαση στο Διαδίκτυο. Οι μαθητές, από την άλλη πλευρά, μπορούν να εμπλουτίσουν τις γνώσεις τους και να βιώσουν την εμπειρία της αλληλεπίδρασης με μια πληθώρα λογισμικών, ενώ τους δίνεται η δυνατότητα να δουλεύουν τις εργασίες τους εκτός σχολικού ωραρίου και να συνεργάζονται με ομάδες μαθητών από άλλα σχολεία. Όλοι έχουν πρόσβαση σε ανεξάντλητους αποθηκευτικούς χώρους και ανεξάντλητη υπολογιστική ισχύ. Άλλα πλεονεκτήματα της χρήσης της τεχνολογίας του «νέφους» είναι και τα εξής:

- Μείωση του χρόνου που απαιτείται από τους υπεύθυνους των σχολικών εργαστηρίων Η/Υ για εγκατάσταση, αναβάθμιση, και ενημέρωση των λογισμικών. Τα λογισμικά πλέον θα διατίθενται από το «νέφος»
- Εξάλειψη της διατήρησης και συντήρησης υψηλής τεχνολογίας σε τοπικό επίπεδο (π.χ. ερευνητικά και εκπαιδευτικά λογισμικά, νέοι επεξεργαστές, μεγαλύτερες μνήμες, κλπ)
- Το «νέφος» δίνει τη δυνατότητα χρήσης εφαρμογών και πόρων που δε διαθέτουμε τοπικά και έτσι μπορούμε πλέον να αξιοποιούμε Η/Υ με υποτυπώδεις δυνατότητες κάτι που συνεπάγεται άμεσα μείωση των δαπανών για την αναβάθμιση και συντήρηση υλικού και λογισμικού των εργαστηρίων Η/Υ (π.χ., μητρικές, σκληροί δίσκοι, μνήμες κλπ).
- Διαθεσιμότητα λογισμικού και δεδομένων. Το λογισμικό μπορεί να χρησιμοποιηθεί οποτεδήποτε και από οποιαδήποτε φορητή συσκευή με δυνατότητα πρόσβασης στο Διαδίκτυο, ενώ εκπαιδευτικοί και εκπαιδευόμενοι

[7] Η Κατανεμημένη Πληροφορική είναι ένας τομέας της επιστήμης της Πληροφορικής που μελετά τα κατανεμημένα συστήματα

έχουν άμεση πρόσβαση στα δεδομένα τους (σημειώσεις, εργασίες, φωτογραφίες, βίντεο), χωρίς να μεριμνούν για τη μεταφορά τους με συσκευές προσωρινής αποθήκευσης (CD's, DVD's, USB flash μνήμες κ.λπ.). [22]

Αναμφισβήτητα τα πλεονεκτήματα από την χρήση του «νέφους» στην εκπαίδευση είναι πολλά. Παρόλα αυτά πολλοί από τους κινδύνους του «νέφους» που αναφέρονται σε επόμενη ενότητα υφίστανται και για πανεπιστημιακά ιδρύματα. Ο Katz [23] περιγράφει ένα σύνολο προβληματισμών που αντανακλούν τον τρόπο με τον οποίο τα πανεπιστημιακά ιδρύματα ανταποκρίνονται στις αλλαγές που το «νέφος» θα επιφέρει στο περιβάλλον της Τεχνολογία Πληροφοριών, στην εκπαίδευση και την συμπεριφορά φοιτητών και προσωπικού. Υπάρχουν πρακτικά ζητήματα που πρέπει να αντιμετωπιστούν - για παράδειγμα, πως μπορεί να εξασφαλιστεί ότι οι πληροφορίες αποθηκεύονται μπορούν να ελέγχονται στο «νέφος»- και φιλοσοφικά ζητήματα- όπως η μορφή της υποτροφίας στον ψηφιακό κόσμο. Τα εκπαιδευτικά ιδρύματα πρέπει να αναγνωρίσουν πως οι αλλαγές στην Τεχνολογία Πληροφοριών που συνεπάγεται το «νέφος», θα επηρεάσουν αναπόφευκτα όλους, αν και το χρονικό διάστημα που αυτό θα λάβει χώρα ποικίλει. Τέλος όπως ο Goldstein δηλώνει [24] "*το «νέφος» μπορεί να μειώσει το σύνολο των παραδοσιακών υπηρεσιών που προσφέρει ένα πανεπιστημιακό ίδρυμα, παρόλα αυτά έχει να σταθμίσει ένα πιο πολυσύνθετο σύνολο επιλογών*".

3.6 Έρευνες σχετικά με το «νέφος»

Στην παρούσα ενότητα θα παρουσιάσουμε αποτελέσματα ερευνών που έχουν πραγματοποιηθεί σχετικά με το «νέφος».[25] Να σημειωθεί πως οι έρευνες πραγματοποιήθηκαν κατά την διάρκεια του έτους 2010.

Η εταιρεία ερευνών Gartner πρόσφατα ανακοίνωσε πως η παγκόσμια αγορά υπηρεσιών «νέφους» μέχρι το 2014 θα έχει φτάσει τα 148,8 δις ενώ το 2010 ήταν 68 δις $. Ο Ben Pring, αντιπρόεδρος της Gartner δήλωσε: "*Παρατηρούμε μια επιτάχυνση στην υιοθέτηση του «νέφους» και των υπηρεσιών του από τις επιχειρήσεις, και μια έκρηξη δραστηριότητας καθώς πάροχοι τεχνολογιών εκμεταλλεύονται την αυξανόμενη εμπορική ευκαιρία*". Η εταιρεία εκτιμά πως κατά την διάρκεια των επόμενων 5 ετών, οι επιχειρήσεις θα δαπανήσουν συνολικά 112 δις $ στα μοντέλα υπηρεσιών

Λογισμικό ως Υπηρεσία (SaaS), Πλατφόρμα ως Υπηρεσία (PaaS) και Υποδομή ως Υπηρεσία (IaaS). Σύμφωνα με την Gartner, το μερίδιο των Η.Π.Α. στην παγκόσμια αγορά υπηρεσιών «νέφους» το 2009 ήταν 60% και 58% το 2010. Μέχρι το 2014 θα μειωθεί στο 50% δείχνοντας έτσι την παγκόσμια ώθηση.

Η ελεγκτική εταιρεία KPMG δημοσίευσε τα αποτελέσματα έρευνας που πραγματοποιήθηκε σε στελέχη πληροφορικής την άνοιξη του 2010, και η οποία επισημαίνει πως το «νέφος» θα είναι ο κύριος μοχλός αύξησης των εσόδων τα επόμενα 3 χρόνια. Το 54% των στελεχών κατονόμασε το «νέφος» ως βασικό παράγοντα για την αύξηση των εσόδων από την Τεχνολογία Πληροφοριών, ενώ στην συνέχεια ακολουθούν με 51% οι εφαρμογές για κινητά, και με 43% το client computing και virtualization. Οι επενδύσεις στο «νέφος» καθώς και στις εφαρμογές για κινητά μπορεί να αυξηθεί κατά περισσότερο από 10% κάθε χρόνο, επισημαίνει η KPMG.

Μια άλλη σημαντική έρευνα πραγματοποιήθηκε από την Pew Internet & American Life Project, από την οποία προέκυψε πως το 71% των ηγετών του επιχειρηματικού κόσμου πιστεύουν πως μέχρι το 2020 δεν θα χρησιμοποιούμε πια έναν ηλεκτρονικό υπολογιστή γενικού σκοπού ως το πιο δημοφιλές εργαλείο πληροφορικής. Αντί αυτού θα χρησιμοποιούμε νέους τύπους εφαρμογών «νέφους» και εφαρμογές Διαδικτύου που θα «τρέχουν» στα smartphones. Το πιο καινοτόμο λογισμικό θα υπάρχει σε smartphones, και οι περισσότεροι προγραμματιστές θα εργάζονται σε εφαρμογές web. Ο σημερινός ηλεκτρονικός υπολογιστής θα συνεχίσει να υπάρχει μέχρι το 2020, σύμφωνα με το 71% των ερωτηθέντων. Αλλά θα βρει νέους ρόλους μετατρέποντάς το σε ένα εργαλείο που θα μπορούσε να περιγραφεί ως ψηφιακός κόμβος. Το 27% των ερωτηθέντων δήλωσε πως το «νέφος» θα αναπτυχθεί και θα μπει στην ζωή μας, αλλά ο ηλεκτρονικός υπολογιστής θα εξακολουθεί να είναι η κύρια συσκευή που θα χρησιμοποιούμε για τις υπολογιστικές εργασίες μας. Η έρευνα αναφέρει την φράση "*Διαδίκτυο των Πραγμάτων* (internet of things)", το οποίο θα συνδέει συσκευές που θα έχουν την δική τους διεύθυνση IP. Είτε πρόκειται για συσκευές ελέγχου είτε για το τηλεχειριστήριο της τηλεόρασης, θα παρέχονται μέσω του «νέφους» «έξυπνα» χαρακτηριστικά: για παράδειγμα, εάν χάσεις το τηλεχειριστήριο της τηλεόρασης, μπορείς να χρησιμοποιήσεις το smartphone για να το βρεις, μέσω μιας εφαρμογής.

Το «νέφος» και η υποκείμενη τεχνολογία ωριμάζουν γρήγορα. Υπάρχει μια αίσθηση πως είναι επιτακτική η ανάγκη να ερευνήσει η βιομηχανία τις δυνατότητες που προσφέρονται από το «νέφος». Είναι καιρός λοιπόν οι εταιρείες να ασχοληθούν σοβαρά με τους τρόπους με τους οποίους μπορούν να επωφεληθούν από το «νέφος». Εάν το 2010 είναι η χρονιά που το «νέφος» είδε μια τεράστια αύξηση ενδιαφέροντος λόγω των δυνατοτήτων του, δεν είναι δύσκολο να προβλεφτεί πως το 2011 θα φέρει σημαντικές αλλαγές στον τρόπο με τον οποίο οι επιχειρήσεις θα σχεδιάσουν και θα κατασκευάσουν τις υποδομές πληροφορικής τους.

3.7 Πάροχοι υπηρεσιών «νέφους»

Σήμερα υπάρχουν πολλές εταιρείες που παρέχουν στους πελάτες τους υπηρεσίες «νέφους». Οι κυριότερες από αυτές είναι οι Amazon, Rackspace Cloud, Salesforce, Skytap, Microsoft, Google. Κάποιες από τις μεγαλύτερες εταιρείες Πληροφορικής που δραστηριοποιούνται στο «νέφος» είναι οι Huawei, Cisco, Fujitsu, DC Wirenet, Dell, Red Hat, Hewlett Packard, IBM, VMware, Hitachi και NetApp. Ακολουθεί ένας συγκεντρωτικός πίνακας με τους περισσότερους παρόχους υπηρεσιών «νέφους».

Cloud computing	Cloud storage
Amazon	Amazon S3
Microsoft	Intermap XIPCloud Storage
Flexiant	Nirvanix
Google	Windows Azure
OneNet	PhoneKlone
Joyent	Dropbox
Rackspase Cloud	Box.net
Salesforce	
Skytap	
Jitscale	
Tata IAAS	
DedicatedNow	

Πίνακας 1. Συγκεντρωτικός πίνακας παρόχων υπηρεσιών «νέφους»

3.7.1 Υπηρεσίες «νέφους» της Google

Στην συνέχεια θα περιγράψουμε ενδεικτικά τις υπηρεσίες «νέφους» που προσφέρει η Google. Η εταιρεία Google είναι από τους πρώτες εταιρείες που προσέφεραν υπηρεσίες «νέφους», γι' αυτό άλλωστε έχει πλέον καθιερωθεί στον χώρο. Οι υπηρεσίες που προσφέρει είναι η Google Apps[8], και η Google App Engine[9].

Η Google Apps είναι μια σουίτα που περιλαμβάνει πολλές υπηρεσίες όπως το Gmail, Google Docs, Google Calendar, Google Groups, Google Sites, και Google Video. Το Gmail προσφέρει υπηρεσίες ηλεκτρονικού ταχυδρομείου και το Google Calendar προσφέρει ένα ημερολόγιο με ραντεβού παρόμοιο με εκείνο του Outlook. Υπάρχει δυνατότητα πρόσβασης και μέσω κινητού τηλεφώνου. Με το Google Groups ένας χρήστης μπορεί να δημιουργεί και να διαχειρίζεται ομάδες. Επιπλέον μπορεί να ελέγχει ποιος έχει πρόσβαση στο περιεχόμενο, ενώ τα μέλη μιας ομάδας μπορούν να λαμβάνουν μέρος σε μεταξύ τους συζητήσεις. Μια τέτοια υπηρεσία θα μπορούσε πιθανώς να χρησιμοποιηθεί από τους εργαζόμενους κάποιας επιχείρησης, καθώς δίνει την δυνατότητα διαμοιρασμού έγγραφων, ημερολόγιων, και κοινόχρηστων φακέλων μεταξύ μιας ομάδας χρηστών αντί μεταξύ μεμονωμένων χρηστών.

Το Google Docs είναι μια δωρεάν υπηρεσία που επιτρέπει στους χρήστες να δημιουργούν, να διαμοιράζονται και να συνεργάζονται σε έγγραφα, υπολογιστικά φύλλα και παρουσιάσεις. Επιπλέον ο χρήστης μπορεί να δημιουργήσει φόρμες HTML. Ο χρήστης της υπηρεσίας έχει πρόσβαση στο Google Docs μέσω ενός web browser, δεν απαιτεί ηλεκτρονικά ίχνη και η υπηρεσία είναι έτοιμη για χρήση. Κάποιες μικρές επιχειρήσεις χρησιμοποιούν το Google Docs ως εναλλακτική λύση για το Office. Αν και δεν έχει τόσο πλήρεις δυνατότητες, όπως το Office, το Google Docs παρέχει βασικές δυνατότητες επεξεργασίας κειμένου και λογιστικών φύλλων. Επιτρέπει την εισαγωγή των περισσότερων μορφών εγγράφων του Office συμπεριλαμβανομένων των .doc, .docx, .xls, and .xlsx. Πρόσφατες βελτιώσεις επιτρέπουν επίσης την επεξεργασία του εγγράφου και offline.

Το Google Sites είναι ένας τρόπος να δημιουργήσει κάποιος εύκολα ασφαλείς ιστοσελίδες για intranet και ομαδικά έργα. Δεν απαιτείται προγραμματισμός ούτε

[8] Περισσότερες πληροφορίες στην ηλεκτρονική διεύθυνση www.google.com/apps/intl/en/business/index.html
[9] Περισσότερες πληροφορίες στην ηλεκτρονική διεύθυνση code.google.com/intl/el-GR/appengine/

γνώσεις HTM καθώς προσφέρει έτοιμα πρότυπα. Οι διαχειριστές μπορούν να διαχειριστούν την ιστοσελίδα δίνοντας δικαιώματα χρήσης σε όλη την επιχείρηση, και οι συγγραφείς μπορούν να επιτρέψουν και να ανακαλέσουν την πρόσβαση σε αρχεία οποιαδήποτε στιγμή επιθυμούν.

Με το Google Video οι εργαζόμενοι μπορούν να μοιραστούν βίντεο με τους συναδέλφους τους με ασφάλεια χωρίς να αποκαλύπτονται εμπιστευτικές πληροφορίες. Ο χρήστης επίσης μπορεί να αναρτήσει, να αναπαράγει και να αναζητήσει βίντεο online.

Η υπηρεσία Google Apps κοστίζει 50 $ τον χρόνο για κάθε χρήστη. Υπάρχουν πολλές εκδόσεις συμπεριλαμβανομένων των Standard, Premier, Educators, Non-Profit, και Government.

Η Google προσφέρει επίσης μια υπηρεσία που ονομάζεται Google App Engine που επιτρέπει στους χρήστες να «τρέχουν» web εφαρμογές στους server της Google. Υποστηρίζει Java και Python εφαρμογές. Η Google App Engine επιτρέπει στους χρήστες να δημιουργούν και να φιλοξενούν εφαρμογές web στο ίδιο σύστημα που υποστηρίζει τις Google εφαρμογές. Προσφέρει γρήγορη ανάπτυξη και εγκατάσταση, απλή διαχείριση χωρίς να χρειάζεται ο χρήστης να ασχοληθεί με το υλικό, τα patches[10] ή το back up. Επίσης προσφέρει προσαρμοστικότητα χωρίς ιδιαίτερη προσπάθεια από τον χρήστη.

3.7.2 Η υπηρεσία Pithos

Θα περιγράψουμε στην συνέχεια την υπηρεσία Pithos[11] που βασίζεται στο «νέφος». Η υπηρεσία ανήκει στο Υπουργείο Παιδείας Δια Βίου Μάθησης και Θρησκευμάτων και συγκεκριμένα στην Γενικής Γραμματείας Έρευνας και Τεχνολογίας. Η διαχείρισή της γίνεται από την ΕΔΕΤ Α.Ε., η οποία έχει ως αντικείμενο τη διαχείριση του Εθνικού Δικτύου Έρευνας & Τεχνολογίας κατά το πρότυπο των αντίστοιχων Ερευνητικών και Εκπαιδευτικών Δικτύων της Ευρωπαϊκής Ένωσης.

[10] Ένα patch είναι ένα κομμάτι λογισμικού που έχει σχεδιαστεί για να διορθώνει προβλήματα ή να ενημερώνει (update) ένα πρόγραμμα υπολογιστή ή τα δεδομένα που αυτό υποστηρίζει.
[11] Περισσότερες πληροφορίες στην ηλεκτρονική διεύθυνση pithos.grnet.gr/description.html

Η υπηρεσία Pithos προσφέρει σε κάθε χρήστη 50 GBytes αποθηκευτικού χώρου online, προσβάσιμα από παντού, πάντοτε, με ασφάλεια. Η χρήση της υπηρεσίας είναι ελεύθερη και δωρεάν για τους φοιτητές και όλα τα άλλα μέλη της ελληνικής ακαδημαϊκής κοινότητας. Οι χρήστες μπορούν να αποθηκεύσουν με ασφάλεια τα αρχεία τους και να τα μοιραστούν με άλλους χρήστες. Επιπλέον, η υπηρεσία προσφέρει δυνατότητες αναζήτησης, και αρχειοθέτησης (versioning). Συγκεκριμένα υποστηρίζεται η εξής λειτουργίες:

- Ο προσωπικός χώρος αποθήκευσης μπορεί να οργανωθεί σε ιεραρχικές δομές καταλόγων – υποκαταλόγων
- Πέραν της φυσικής οργάνωσης σε καταλόγους, κάθε αρχείο μπορεί να συσχετιστεί με ένα ή περισσότερα tags για λόγους καλύτερης αρχειοθέτησης και ευκολότερης αναζήτησης
- Υποστηρίζεται αναζήτηση πλήρους κειμένου στα ονόματα, το περιεχόμενο και στα tags των αρχείων
- Υποστηρίζεται "καλάθι αχρήστων" (trash bin) με δυνατότητα επαναφοράς σβησμένων αρχείων
- Επιλεκτικά για ένα αρχείο το σύστημα μπορεί να διατηρεί ιστορικό αλλαγών (versions) – σε αυτή την περίπτωση το μέγεθος όλων των αρχείων υπολογίζεται στο όριο αποθήκευσης του χρήστη
- Ένα αρχείο ή ένας κατάλογος μπορεί να γίνει διαθέσιμο σε άλλους χρήστες της υπηρεσίας, με δικαίωμα ανάγνωσης μόνο, τροποποίησης ή ακόμη και τροποποίησης δικαιωμάτων. Επίσης, ένα αρχείο μπορεί να γίνει διαθέσιμο για ανάκτηση εκτός συστήματος (unauthenticated download).

Για την πρόσβαση στην υπηρεσία Pithos το μόνο που χρειάζεται από τους χρήστες είναι να έχουν λογαριασμό (account) σε Πανεπιστήμιο, Πολυτεχνείο ή ΑΤΕΙ. Μπορεί ο χρήστης να χρησιμοποιήσει την υπηρεσία με τρεις τρόπους:

- Μέσω ενός φυλλομετρητή (browser).
- Μέσω ανεξάρτητης εφαρμογής (standalone rich client)
- Μέσω Firefox plugin

Από την πλευρά του Ιδρύματος στο οποίο ανήκει ο χρήστης, η μόνη απαίτηση είναι να είναι συνδεμένο με την υποδομή Shibboleth του Εθνικού Δικτύου Έρευνας και Τεχνολογίας. Η υπηρεσία Pithos βρίσκεται αυτή τη στιγμή σε φάση δοκιμών (beta

testing), είναι σταθερή και διαθέσιμη στους χρήστες της. Παρέχεται online εγχειρίδιο χρήσης, και λειτουργεί forum και υπηρεσία support για επίλυση απορίων και τεχνική υποστήριξη. Επίσης παρέχεται φόρμα όπου ο χρήστης μπορεί να αναφέρει κάθε πιθανή παραβίαση των όρων χρήσης. Τέλος έχει υλοποιηθεί με το λογισμικό GRNET Storage Service (GSS), το οποίο είναι διαθέσιμο με άδεια ανοιχτού κώδικα.

3.8 Οφέλη και ζητήματα προς επίλυση

Στην παρούσα ενότητα γίνεται μια προσπάθεια να παρουσιαστούν εν συντομία πλεονεκτήματα καθώς και πιθανά οφέλη αλλά και μειονεκτήματα, προκλήσεις και πιθανοί κίνδυνοι από την χρήση του «νέφους» σε εταιρικά περιβάλλοντα αλλά και από ιδιώτες. Σαφώς τα παρακάτω δεν είναι τα μοναδικά, διότι το «νέφος» είναι ένα νέο αντικείμενο στον χώρο της Πληροφορικής το οποίο εξελίσσεται ραγδαία με την πάροδο του χρόνου, και προκύπτουν καινούρια δεδομένα συνεχώς.

Θα ξεκινήσουμε με τα οφέλη [26]:

- **Τιμολόγηση υπηρεσίας**: Οι χρήστες της πλατφόρμας καταναλώνουν υπολογιστικές και αποθηκευτικές υπηρεσίες on-demand. Πληρώνουν για όσο τις χρησιμοποιούν και συγκεκριμένα όσο αφορά εταιρείες, με χρήματα από τον προϋπολογισμό για τις λειτουργικές δαπάνες (OPEX), αντί να πληρώνουν εξ αρχής για πόρους που θα άνηκαν στις κεφαλαιακές δαπάνες (CAPEX). Για πολλές νέες επιχειρήσεις το «νέφος» προσφέρει υπολογιστικούς πόρους που διαφορετικά θα ήταν δύσκολο να έχουν. Το μετρούμενο κόστος και η προσέγγιση pay-per-use προσελκύει πολλές μικρές και μεσαίες επιχειρήσεις. Η διαχείριση και η συντήρηση της υποδομής γίνεται εξ αποστάσεως, συνήθως με μια μηνιαία χρέωση. Επιτρέποντας να αγοράσουν μόνο υπηρεσίες που χρειάζονται, αντί να επενδύουν σε πολύπλοκες και δαπανηρές υποδομές, οι εταιρείες μπορούν να μειώσουν τα κόστη για την ανάπτυξη, δοκιμή και συντήρηση νέων και υπαρχόντων συστημάτων.
- **Προσαρμοστικότητα**: Το μεγάλο πλεονέκτημα του «νέφους» είναι η προσαρμοστικότητα: η δυνατότητα δηλαδή να προσθέτουμε χωρητικότητα ή εφαρμογές σχεδόν στιγμιαία. Οι εταιρείες αγοράζουν ακριβώς το ποσό της μνήμης και υπολογιστικής ισχύος που χρειάζονται και μπορούν να

πληρώσουν, σε επίπεδο υπηρεσίας που καθορίζεται με τον κατασκευαστή-πωλητή, με δυνατότητες που μπορούν να προστεθούν ή να αφαιρεθούν κατά βούληση. Οι χρήστες μπορούν να αυξήσουν ή να μειώσουν το επίπεδο χρήσης των υπολογιστικών πόρων και των υπηρεσιών ευέλικτα και εύκολα. Το «νέφος» διαφέρει από τις περισσότερες μορφές κατανεμημένων συστημάτων πληροφορικής στον τρόπο με τον οποίο κλιμακώνει "προς τα κάτω" ή "προς τα πάνω" τους υπολογιστικούς και αποθηκευτικούς πόρους. Οι χρήστες αντί να εκμεταλλεύονται ένα συγκεκριμένο σύνολο πόρων, μπορούν να προσθέτουν ή να αφαιρούν χωρητικότητα κατά βούληση, σχεδόν στιγμιαία, και πληρώνουν μόνο γι' αυτό που πραγματικά χρησιμοποιούν.

- **Ιδεατοί πόροι**: Το «νέφος» δεν θα ήταν εφικτό χωρίς την μέθοδο virtualization, όχι για τεχνικούς λόγους, αλλά εξαιτίας της προφανής απαίτησης των επιχειρήσεων: την ανάγκη για multi-tenancy. Το «νέφος» στηρίζεται στον διαμοιρασμό μιας κοινής υποδομής από πολλαπλές ομάδες χρηστών που συχνά αναφέρονται ως μισθωτές (tenants). Η αρχιτεκτονική multi-tenancy μπορεί να επιτευχθεί μόνο μέσω ενός είδους virtualization, είτε σε επίπεδο βάσης δεδομένων (Salesforce.com), είτε σε επίπεδο CPU (Amazon EC2), είτε σε επίπεδο πυρήνα λειτουργικού συστήματος (Red Hat), είτε τέλος σε επίπεδο server εφαρμογών (application server). Σε αντίθεση με το grid computing, όπου συγκεντρώνονται και συναθροίζονται κατανεμημένοι υπολογιστικοί πόροι για τον χειρισμό πολύ μεγάλων εργασιών που θα κατανάλωναν πάρα πολύ χρόνο και χώρο για να ολοκληρωθούν σ' έναν μόνο server, το «νέφος» δημιουργεί εικονικά κομμάτια των πόρων από συστοιχίες server και αποθηκευτικές συσκευές, με ιδανικό μέγεθος ώστε να καλύπτουν τις ανάγκες των χρηστών. Αυτοί οι εικονικοί πόροι μπορεί να είναι λίγοι ή πολλοί, και να κλιμακώνονται καθώς αλλάζουν οι ανάγκες των χρηστών με την πάροδο του χρόνου.
- **Αυτοματοποίηση της διαχείρισης:** Οι πλατφόρμες «νέφους» διαφέρουν από τα παραδοσιακά κέντρα δεδομένων εταιρειών σ' ένα σημαντικό στοιχείο: την τυποποίηση. Ενώ ένα τυπικό κέντρο δεδομένων συνήθως φιλοξενεί κάθε έκδοση λειτουργικού συστήματος και βάσεων δεδομένων, δημιουργώντας έτσι τεράστια έξοδα διαχείρισης, οι περισσότερες πλατφόρμες «νέφους» τυποποιούν ένα μόνο είδος CPU, έναν hypervisor (VMware, Xen, κλπ.), ένα

μόνο λειτουργικό σύστημα (κάποια έκδοση του Linux συνήθως), και μία μόνο βάση δεδομένων (συνήθως SQL). Η τυποποίηση αυτή έχει ένα προφανές όφελος για τις επιχειρήσεις: δραματική μείωση των λειτουργικών δαπανών.

- **Self-service παροχή υπηρεσιών:** Το «νέφος» και το Λογισμικό ως Υπηρεσία (Software as a Service) συχνά συγκρίνονται με το μοντέλο Application Service Provider (ASP)[12] που ήταν δημοφιλές για ένα σύντομο χρονικό διάστημα στα τέλη της δεκαετίας του ’90. Όμως ένα σημαντικό στοιχείο τα διαφοροποιεί θεμελιωδώς: την δυνατότητα παροχής υπηρεσιών χωρίς βοήθεια. Με το μοντέλο ASP έπρεπε να παρέχονται σε κάθε πελάτη εξειδικευμένοι servers[13], κάτι το οποίο σήμαινε πως θα έπρεπε να περιλαμβάνονται τεχνικοί πόροι κάθε φορά που θα εγγραφόταν ένας νέος πελάτης. Ο λογαριασμός θα αυξανόταν από τα μεγάλα τέλη εγκατάστασης ενώ η υπηρεσία θα γινόταν διαθέσιμη για λειτουργία στην καλύτερη περίπτωση μέσα σε λίγες μέρες. Με το «νέφος» οι επιχειρήσεις και οι τελικοί χρήστες μπορούν να παρέχουν εφαρμογές και λογαριασμούς χρηστών με μόνο μερικά κλικ του ποντικιού, και όλα αυτά γίνονται αμέσως διαθέσιμα.
- **Ιδιοκτησιακό καθεστώς από τρίτους:** Το «νέφος» είναι μια νέα μορφή outsourcing[14]. Οι πελάτες που προσπαθούν να επικεντρώσουν την κατανομή των περιορισμένων κεφαλαίων τους στις βασικές δραστηριότητές τους, σύντομα αντιλαμβάνονται τα οφέλη απομάκρυνσης της IT υποδομής εκτός ισολογισμού τους. Επιπλέον, καθώς η τεχνολογία εξελίσσεται και οι πάροχοι υπηρεσιών αναπτύσσουν όλο και μεγαλύτερα κέντρα δεδομένων, η απόκτηση και λειτουργία κέντρων δεδομένων τελευταίας τεχνολογίας έχει όλο και λιγότερο νόημα από οικονομικής άποψης για τους περισσότερους οργανισμούς. Το «νέφος» σχετίζεται με την μεταβίβαση της ιδιοκτησίας τέτοιων πόρων σε τρίτους που ειδικεύονται στην διαχείρισή τους.

[12] Ένας πάροχος υπηρεσιών εφαρμογών (Application Service Provider -ASP) είναι μια επιχείρηση που παρέχει υπηρεσίες βασισμένες σε υπολογιστή μέσω ενός δικτύου. Το λογισμικό που παρέχεται χρησιμοποιώντας ένα ASP μοντέλο μερικές φορές καλείται on-demand λογισμικό ή Λογισμικό ως Υπηρεσία (SaaS). Τέτοιες επιχειρήσεις περιορίζονται στο να παρέχουν πρόσβαση σε συγκεκριμένα προγράμματα εφαρμογών χρησιμοποιώντας συγκεκριμένο πρωτόκολλο, όπως το HTTP.

[13] Είναι μια μορφή Internet hosting όπου ο πελάτης μισθώνει έναν server χωρίς να τον μοιράζεται με κανέναν άλλον.

[14] Το outsourcing συχνά αναφέρεται στην διαδικασία σύναψης συμβολαίου με τρίτους. Περιλαμβάνει συνήθως την ανάθεση μιας επιχειρηματικής λειτουργίας – που συνήθως πραγματοποιείται στο εσωτερικό της επιχείρησης- σε έναν εξωτερικό πάροχο.

- **Διαχειρίσιμες λειτουργίες:** Το «νέφος» συνηγορεί υπέρ ενός μοντέλου σύμφωνα με το οποίο η υποδομή IT δεν ανήκει μόνο σε έναν τρίτο, αλλά την διαχειρίζεται κιόλας. Ενημερώσεις λογισμικού, δημιουργία αντιγράφων ασφαλείας και αμέτρητες άλλες εργασίες που απαιτούνται για τη διαχείριση των κρίσιμων επιχειρηματικών εφαρμογών σε καθημερινή βάση γίνεται ευθύνη του τρίτου μέρους, σύμφωνα με τις *Συμφωνίες Επιπέδου Υπηρεσιών* (Service Level Agreements).
- **Πρόσβαση**: Το «νέφος» υπόσχεται πρόσβαση σε υψηλής ισχύος υπολογιστικούς και αποθηκευτικούς πόρους σε οποιονδήποτε διαθέτει μια συσκευή με πρόσβαση στο διαδίκτυο. Παρέχοντας τέτοιες δυνατότητες βοηθά την διευκόλυνση πρωτοβουλιών τηλεργασίας.
- **Συνεργασία**: Το «νέφος» προσφέρει ένα περιβάλλον όπου οι χρήστες μπορούν να αναπτύξουν υπηρεσίες βασισμένες στο λογισμικό, το οποίο προάγει την συνεργασία και προωθεί ευρύτερη ανταλλαγή πληροφοριών, όχι μόνο στο εσωτερικό του οργανισμού αλλά και μεταξύ ιδιωτών και κυβερνητικών φορέων.
- **Αυξημένη υπολογιστική ισχύς**: Όταν κάποιος χρήστης είναι συνδεδεμένος στο σύστημα του «νέφους», έχει στην διάθεσή του την υπολογιστική ισχύ ολόκληρου του «νέφους». Δεν είναι πλέον περιορισμένος μόνο σε ότι μπορεί να κάνει με τον υπολογιστή του, αλλά μπορεί να εκτελέσει εργασίες χρησιμοποιώντας την υπολογιστική ισχύ χιλιάδων υπολογιστών και server. Με άλλα λόγια στο «νέφος» μπορεί να επιχειρήσει μεγαλύτερες και δυσκολότερες εργασίες απ' ότι στον υπολογιστή του.
- **Απεριόριστη αποθηκευτική χωρητικότητα**: Το «νέφος» προσφέρει σχεδόν απεριόριστη αποθηκευτική χωρητικότητα. Ας σκεφτούμε όταν εξαντλείται ο αποθηκευτικός χώρος του υπολογιστή γραφείου ή του φορητού υπολογιστή. Τα 250GB του σκληρού δίσκου του υπολογιστή μας μοιάζουν ελάχιστα σε σχέση με τα εκατοντάδες petabytes (ένα εκατομμύριο gigabytes) που διατίθενται στο «νέφος». Μπορεί κάποιος να αποθηκεύσει οτιδήποτε θελήσει.
- **Αποδέσμευση από συγκεκριμένες συσκευές:** Όταν κάποιος βρίσκεται στο «νέφος», δεν είναι πλέον δεσμευμένος μ' έναν μόνο υπολογιστή ή δίκτυο. Δεν χρειάζεται να αγοράσει μια συγκεκριμένη έκδοση ενός προγράμματος για κάποια συσκευή ή να αποθηκεύσει κάποιο έγγραφο σε μια συγκεκριμένη

μορφή ώστε να είναι συμβατό με μια συσκευή. Προγράμματα και αρχεία που δημιουργεί κάποιος με αυτά, παραμένουν ίδια ανεξάρτητα από ποιόν υπολογιστή χρησιμοποιεί.

- **Διαθεσιμότητα:** Οι πάροχοι υπηρεσιών «νέφους» έχουν την υποδομή και το εύρος ζώνης να καλύψουν τις απαιτήσεις των επιχειρήσεων για πρόσβαση υψηλής ταχύτητας, μνήμη και εφαρμογές. Δεδομένου ότι αυτοί οι πάροχοι έχουν άφθονα μονοπάτια (paths), η δυνατότητα για εξισορρόπηση φορτίου εξασφαλίζει πως τα συστήματα δεν θα υπερφορτωθούν και οι υπηρεσίες δεν θα καθυστερούν.
- **Ειδίκευση:** Είναι πολλές οι ειδικές γνώσεις που θα πρέπει να έχει κάποιος για να δημιουργήσει και να λειτουργήσει συστήματα ώστε να περιλαμβάνουν ασφάλεια, δυνατότητα κλιμάκωσης, συντήρηση της πλατφόρμας, backup δεδομένων και άλλα. Σ' ένα παραδοσιακό μοντέλο, κάθε αναπτυξιακή προσπάθεια θα έπρεπε να ενσωματώνει αυτή την ειδικευμένη γνώση στο προσωπικό της εταιρείας ή του οργανισμού. Το «νέφος» επιτρέπει αυτές οι δυνατότητες να επανδρωθούν από ειδικούς οι οποίοι μπορούν να διαμοιράζονται μεταξύ πολλών πελατών. Αντί να προσλαμβάνεται ένα πρόσωπο που κάνει αξιοπρεπή δουλειά σε όλα αυτά τα αντικείμενα, οι πάροχοι των υπηρεσιών μπορούν να προσλάβουν άτομα με μεγάλη ειδίκευση σε κάθε αντικείμενο, και στην συνέχεια να αποσβέσουν το κόστος κατανέμοντάς το σ' ένα μεγάλο αριθμό πελατών.

Οφέλη	Περιγραφή
Τιμολόγηση υπηρεσίας	**Οι χρήστες πληρώνουν μόνο για όσο χρησιμοποιούν τις υπηρεσίες**
Προσαρμοστικότητα	**Οι χρήστες μπορούν να αυξήσουν ή να μειώσουν το επίπεδο χρήσης των υπολογιστικών πόρων & των υπηρεσιών ευέλικτα & εύκολα**
Virtualized πόροι	**Εξαιτίας της ανάγκης για multi-tenancy το «νέφος» δεν θα ήταν εφικτό χωρίς την μέθοδο virtualization**
Αυτοματοποίηση της διαχείρισης	**Οι πλατφόρμες «νέφους» διαφέρουν από τα παραδοσιακά κέντρα δεδομένων στην ύπαρξη τυποποίησης**
Self-service παροχή υπηρεσιών	**Δυνατότητα παροχής υπηρεσιών χωρίς βοήθεια**
Ιδιοκτησιακό καθεστώς από τρίτους	**Μεταβίβαση της ιδιοκτησίας πόρων σε**

	τρίτους που ειδικεύονται στην διαχείρισή τους
Διαχειρίσιμες λειτουργίες	**Η διαχείριση της υποδομής γίνεται από "τρίτα μέρη"**
Πρόσβαση	**Πρόσβαση σε πόρους για οποιονδήποτε διαθέτει μια συσκευή με πρόσβαση στο Διαδίκτυο**
Συνεργασία	**Προάγει την συνεργασία & προωθεί την ευρύτερη ανταλλαγή πληροφοριών**
Αυξημένη υπολογιστική ισχύς	**Ο χρήστης μπορεί να εκτελέσει δυσκολότερες υπολογιστικές εργασίες χρησιμοποιώντας την υπολογιστική ισχύ χιλιάδων υπολογιστών & server**
Απεριόριστη αποθηκευτική χωρητικότητα	**Το «νέφος» προσφέρει σχεδόν απεριόριστη αποθηκευτική χωρητικότητα**
Αποδέσμευση από συγκεκριμένες συσκευές	**Αποδέσμευση από έναν μόνο υπολογιστή ή δίκτυο, από συγκεκριμένη έκδοση ενός προγράμματος για κάποια συσκευή ή αποθήκευση κάποιου έγγραφο σε μια συγκεκριμένη μορφή ώστε να είναι συμβατό με μια συσκευή**
Διαθεσιμότητα	**Οι πάροχοι έχουν την υποδομή & το εύρος ζώνης να καλύψουν τις απαιτήσεις των χρηστών για πρόσβαση υψηλής ταχύτητας, μνήμη & εφαρμογές**
Ειδίκευση	**Γνώσεις ειδικευμένων διαμοιράζονται μεταξύ πολλών πελατών**

Πίνακας 2. Συγκεντρωτικός πίνακας οφελών του «νέφους»

Στην συνέχεια ακολουθούν τα ζητήματα προς επίλυση:

- **Έλλειψη προτύπων αγοράς**: Το «νέφος» βρίσκεται στο αρχικό στάδιο της ανάπτυξής του και συνέπεια αυτού είναι η έλλειψη οριστικών προτύπων αγοράς. Επίσης υπάρχει ένα ρεύμα νεοεισερχομένων στην βιομηχανία, και κάθε ένας από αυτούς προσπαθεί να κερδίσει μερίδιο αγοράς. Ενώ η αγορά βρίσκεται σε ρευστότητα, τυχόν αποφάσεις για δέσμευση μ' έναν συγκεκριμένο πάροχο, ενδέχεται να έχει αρνητικές συνέπειες καθώς η αγορά ωριμάζει. Όλοι οι πάροχοι υπηρεσιών χρησιμοποιούν διαφορετικά πρότυπα και διαφορετικές τεχνολογίες (π.χ. η μηχανή αποθήκευσης της Azure δεν

χρησιμοποιεί μια συγκεκριμένη σχεσιακή βάση δεδομένων, η υποδομή αποθήκευσης της Amazon είναι διαφορετική από εκείνη ενός τυπικού κέντρου δεδομένων). Έτσι δεν μπορούμε να μεταφέρουμε εφαρμογές στο «νέφος» και απλά να περιμένουμε να εκτελεστούν. Επιπλέον είναι σχεδόν απίθανο τα «νέφη» διαφορετικών παρόχων να είναι διαλειτουργικά. Το Open Grid Forum αναπτύσσει ένα Open Cloud Computing Interface για να επιλυθεί το συγκεκριμένο ζήτημα, και το Open Cloud Consortium εργάζεται πάνω στα standard. Τα ευρήματα αυτών των ομάδων θα πρέπει να ωριμάσουν, αλλά δεν είναι γνωστό αν θα καλύψουν τις ανάγκες των ανθρώπων που χρησιμοποιούν τις υπηρεσίες αυτές αλλά και τις διεπαφές που αυτές οι υπηρεσίας χρειάζονται.

- **Ποιότητα υπηρεσιών (Quality of Service- QoS):** τα παρακάτω ζητήματα αφορούν την ποιότητα υπηρεσιών «νέφους». Καταρχήν το «νέφος» είναι απλά αδύνατο χωρίς σύνδεση στο Διαδίκτυο. Εάν δεν έχεις σύνδεση δεν μπορείς να έχεις πρόσβαση σε τίποτα, ακόμα και στα έγγραφά σου. Ομοίως το «νέφος» δεν λειτουργεί καλά με χαμηλές ή ευρυζωνικές ταχύτητες. Οπότε προκύπτουν ζητήματα απόδοσης. Ακόμα όμως και με μια γρήγορη σύνδεση, web-based εφαρμογές μπορεί να είναι πιο αργές από τις αντίστοιχες του υπολογιστή μας. Αυτό συμβαίνει γιατί τα πάντα σχετικά με το πρόγραμμα, από το interface μέχρι το έγγραφο στο οποίο εργαζόμαστε, θα πρέπει να σταλούν και να επιστρέψουν από τον υπολογιστή μας στους υπολογιστές του «νέφους» και αντίστροφα. Εάν το δίκτυο είναι αργό εκείνη την στιγμή, δεν θα έχουμε στιγμιαία πρόσβαση όπως έχουμε συνηθίσει με τις εφαρμογές του υπολογιστή μας. Επιπρόσθετα, το υλικό ελέγχεται από τον πάροχο της υπηρεσίας, και όχι από κάποιον επιστήμονα, οπότε η κατανομή και ανακατανομή των υπολογιστών μπορεί να επηρεάσει τους χρόνους εκτέλεσης. Το να δεσμεύεται κάποιος πελάτης μ' ένα συγκεκριμένο πάροχο δημιουργεί θέματα αξιοπιστίας. Έχουν υπάρξει προβλήματα πρόσβασης στο «νέφος» από μεγάλες εταιρείες, όπως η Google και η Amazon, αν και συνήθως είναι προσωρινά για μερικές ώρες. Ωστόσο θα πρέπει να είναι πλεονέκτημα του «νέφους» να μην ανησυχούν οι χρήστες του για τέτοιου είδους προβλήματα, αν και αυτό δεν είναι εφικτό ακόμα Τέλος, μπορεί να μην είναι εύκολο να προσαρμοστούν οι Συμφωνίες Επιπέδου Υπηρεσιών με τις ειδικές ανάγκες μιας επιχείρησης. Η αποζημίωση για νεκρούς χρόνους μπορεί να είναι ανεπαρκής και οι

Συμφωνίες Επιπέδου Υπηρεσιών είναι απίθανο να καλύψουν τις επακόλουθες ζημίες. Τέλος, όσο αφορά τους παρόχους και τις επιχειρήσεις-πελάτες η υπάρχουσα νομοθεσία σχετικά με το «νέφος» είναι ελλιπής. Η συμμόρφωση με τους κανονισμούς και τους νόμους σε διαφορετικές γεωγραφικές περιοχές μπορεί να είναι μια πρόκληση για τις επιχειρήσεις. Προς το παρόν υπάρχει ελάχιστη νομική κάλυψη σχετικά με το ποιος έχει την ευθύνη στο «νέφος». Είναι σημαντικό να εξασφαλιστεί μέσα από το συμβόλαιο με τον πάροχο ποιες είναι οι περιοχές που είναι υπεύθυνος και υπόλογος για όλα τα θέματα που πιθανώς θα προκύψουν.

- **Ασφάλεια-Ιδιωτικότητα**: Ίσως δύο από τα πιο καυτά ζητήματα που αφορούν το «νέφος» σχετίζονται με την αποθήκευση και ασφάλεια των δεδομένων καθώς και την παρακολούθηση της χρήσης του «νέφους» από τον πάροχο. Αυτά τα θέματα επιβραδύνουν την ανάπτυξη των υπηρεσιών. Για να υιοθετηθεί ευρέως το «νέφος» θα πρέπει να υπάρχουν εγγυήσεις πως τα δεδομένα δεν είναι μόνο πάντα προσβάσιμα, αλλά και απόλυτα ασφαλή. Κάθε σημαντική παραβίαση σε δεδομένα θα επιδεινώσει τις ήδη υπάρχουσες ανησυχίες σχετικά με το αν τα δεδομένα στο «νέφος» είναι προστατευμένα. Στο «νέφος», ένα κέντρο δεδομένων περιέχει πληροφορίες που τελικοί χρήστες θα είχαν παραδοσιακά αποθηκεύσει στους υπολογιστές τους. Αυτό προκαλεί ανησυχίες σχετικά με την προστασία της ιδιωτικότητας διότι οι χρήστες πρέπει να αναθέσουν σε τρίτους τα δεδομένα τους. Αλλά πόσο ασφαλές είναι αυτό; Μπορούν μη εξουσιοδοτημένοι χρήστες να αποκτήσουν πρόσβαση σε απόρρητα δεδομένα; Επιπλέον, η μετάβαση σε συγκεντρωτικές υπηρεσίες θα μπορούσε να επηρεάσει την ιδιωτικότητα και την ασφάλεια στις αλληλεπιδράσεις μεταξύ των χρηστών. Απειλές για την ασφάλεια μπορεί να συμβούν κατά την διάρκεια εκτέλεσης κατανεμημένων εφαρμογών. Επιπλέον, είναι πιθανό να προκύψουν και νέες απειλές. Για παράδειγμα, hackers μπορούν να χρησιμοποιήσουν την virtualized υποδομή ως ορμητήριο για νέες επιθέσεις. Οι υπηρεσίες «νέφους» πρέπει να διαφυλάξουν την ακεραιότητα των δεδομένων και την ιδιωτικότητα του χρήστη. Ταυτόχρονα θα πρέπει να ενισχυθεί η διαλειτουργικότητα ανάμεσα στους διάφορους παρόχους υπηρεσιών. Σε αυτό το πλαίσιο, θα πρέπει να διερευνηθούν νέοι μηχανισμοί προστασίας δεδομένων για διασφαλιστεί η ιδιωτικότητα των δεδομένων, η ασφάλεια των πόρων και τα πνευματικά δικαιώματα του

περιεχομένου. Παραδείγματα απειλών ασφάλειας και ιδιωτικότητας είναι τα εξής: 1) οι περισσότεροι πάροχοι IaaS δίνουν στους πελάτες τους την δυνατότητα με μια έγκυρη πιστωτική κάρτα να εγγραφούν και να αρχίσουν να χρησιμοποιούν την υπηρεσία αμέσως. Εκμεταλλευόμενοι τη σχετική ανωνυμία πίσω από τα αυτά τα μοντέλα χρήσης και εγγραφής, οι spammers, οι συγγραφείς κακόβουλου κώδικα και άλλοι εγκληματίες μπορούν να δρουν με σχετική ατιμωρησία 2) οι πάροχοι υπηρεσιών εκθέτουν ένα σύνολο διεπαφών λογισμικού ή API[15] που οι πελάτες χρησιμοποιούν για να αλληλεπιδράσουν με τις υπηρεσίες του «νέφους». Η ασφάλεια και η διαθεσιμότητα των υπηρεσιών εξαρτάται από την ασφάλεια αυτών των βασικών API. Από πιστοποίηση ταυτότητας και έλεγχο πρόσβασης μέχρι κωδικοποίηση, αυτές οι διεπαφές πρέπει να είναι σχεδιασμένες ώστε να παρέχουν προστασία σε ακούσιες ή κακόβουλες προσπάθειες για παράκαμψη της πολιτικής 3) ένα άλλο πρόβλημα αφορά την απώλεια ή διαρροή δεδομένων. Τι γίνεται στην περίπτωση που χαθούν τα δεδομένα που βρίσκονται στο «νέφος» και δεν υπάρχουν τοπικά αντίγραφα (εκτός αν κάποιος μεθοδικά αποθηκεύει όλα του τα έγγραφα και στον υπολογιστή του-κάτι που λίγοι χρήστες κάνουν); Υπάρχουν πολλοί τρόποι για να τεθούν σε κίνδυνο τα δεδομένα. Στο «νέφος» δεν μπορεί να έχει κάποιος χρήστης το είδος ελέγχου των δεδομένων του που χρειάζεται ή την δυνατότητα να αλλάξει ή να ελέγξει τις διαδικασίες ή τις πολιτικές κάτω από τις οποίες οι χρήστες πρέπει να εργάζονται. Διάφορα μέρη μιας εφαρμογής μπορεί να βρίσκονται σε διαφορετικά σημεία μέσα στο «νέφος». Υπάρχουν εργαλεία διαχείρισης συστημάτων για το «νέφος» αλλά δεν είναι ενοποιημένα με υπάρχοντα εργαλεία διαχείρισης συστημάτων, οπότε πιθανώς θα απαιτούνται δυο συστήματα. Οι χρήστες μπορεί να χάσουν τον έλεγχο των δεδομένων τους επειδή εργαλεία που «βλέπουν» ποιος τα χρησιμοποιεί ή ποιος μπορεί να τα «δει» είναι ανεπαρκή. [25] [26]

[15] Ένα Application Programming Interface (API) είναι ένα συγκεκριμένο σύνολο κανόνων και προδιαγραφών που ένα πρόγραμμα λογισμικού μπορεί να ακολουθήσει για να έχει πρόσβαση και να χρησιμοποιεί τις υπηρεσίες και τους πόρους που παρέχονται από ένα άλλο συγκεκριμένο πρόγραμμα που υλοποιεί το API.

Ζητήματα προς επίλυση	Περιγραφή
Έλλειψη προτύπων αγοράς	**Δεν υπάρχουν κοινά πρότυπα αγοράς για όλους του παρόχους υπηρεσιών, τα «νέφη» δεν είναι διαλειτουργικά**
Ποιότητα υπηρεσιών	**Κάποια από τα ζητημάτων είναι: α) εξαρτάται πλήρως από την σύνδεση που διαθέτουμε β) η δέσμευση μ' έναν πάροχο μπορεί να δημιουργήσει θέματα αξιοπιστίας γ) ελλιπής νομοθεσία**
Ασφάλεια-Ιδιωτικότητα	**Δυο από τα πιο σημαντικά ζητήματα**

Πίνακας 3. Συγκεντρωτικός πίνακας ζητημάτων προς επίλυση του «νέφους»

3.9 Chromebook

Το Cromebook αποτελεί μια ακόμα απόδειξη πως το «νέφος» είναι εδώ. Είναι φορητός υπολογιστής που "τρέχει" το λειτουργικό σύστημα Chrome OS της Google και υπόσχεται ταχύτητα, ασφάλεια και υψηλή αυτονομία. Στην πραγματικότητα ο υπολογιστής προωθεί τις υπηρεσίες και την φιλοσοφία της Google και ειδικά τις υπηρεσίες «νέφους». Κάποια από τα χαρακτηριστικά του είναι πως αμέσως μετά την εκκίνηση συνδέεται με ασύρματο δίκτυο, οι εφαρμογές, τα έγγραφα και οι ρυθμίσεις του χρήστη είναι αποθηκευμένα στο «νέφος» οπότε εάν ο χρήστης χάσει τον υπολογιστή του ή χαλάσει μπορεί να χρησιμοποιήσει κάποιο άλλο Cromebook για να έχει πρόσβαση στα δεδομένα του, "τρέχει" εκατομμύρια εφαρμογές πολλές από τις οποίες ο χρήστης μπορεί να χρησιμοποιήσει ακόμα και αν δεν είναι συνδεδεμένος και τέλος οι ενημερώσεις γίνονται αυτόματα χωρίς την παρέμβαση του χρήστη. Επίσης υπάρχει και η δυνατότητα να χρησιμοποιήσουν τις δυνατότητες του Cromebook και άλλοι χρήστες πέραν του ιδιοκτήτη χωρίς όμως να έχουν πρόσβαση στο email ή τα προσωπικά δεδομένα του (Guest Mode). Όσο αφορά την ασφάλεια η εταιρεία υποστηρίζει πως το λειτουργικό σύστημα έχει κατασκευαστεί για να αμύνεται σε συνεχιζόμενες απειλές από malware και ιούς, ενώ υποστηρίζει πολλαπλά επίπεδα προστασίας χρησιμοποιώντας μεταξύ άλλων κρυπτογράφηση δεδομένων και επαλήθευση κατά την εκκίνηση. Επιπλέον το Chromebook έχει και ορισμένα πολύ

ενδιαφέροντα τεχνικά χαρακτηριστικά όπως για παράδειγμα, ότι είναι έτοιμο για χρήση μόλις 8 δευτερόλεπτα μετά το πάτημα του κουμπιού έναρξης λειτουργίας και σε σχέση με τους συμβατικούς φορητούς υπολογιστές και τα netbooks που έχουν αυτονομία γύρω στις 3-4 ώρες το Chromebook υπόσχεται αυτονομία 6-8.5 ωρών.[27]

Η πολιτική απορρήτου του Chromebook βασίζεται στην πολιτική απορρήτου που έχει καθιερώσει η εταιρεία για το Google Chrome (μιας και το Chrome OS είναι χτισμένο γύρω από το Google Chrome). Στην σχετική σελίδα αναφέρεται πως το Chrome OS αποθηκεύει πληροφορίες για τις ρυθμίσεις του φυλλομετρητή (όπως δεδομένα για τους σελιδοδείκτες) στους διακομιστές της Google πάντοτε σε σχέση με τον λογαριασμό Google του χρήστη. Αναφέρεται πως ο χρήστης μπορεί να ρυθμίσει αυτές τις πληροφορίες από τον πίνακα ελέγχου, ενώ οι πληροφορίες που συγκεντρώνονται από τον λογαριασμό Google του χρήστη προστατεύονται από την πολιτική απορρήτου της Google. Επιπλέον το λειτουργικό σύστημα θα συγκεντρώνει στατιστικά στοιχεία χρήσης και αναφορές σφαλμάτων (εκτός αν ο χρήστης απενεργοποιήσει την συγκεκριμένη επιλογή) τα οποία όπως αναφέρει η εταιρεία είναι μη προσωπικές πληροφορίες (όπως π.χ. πόσο συχνά συμβαίνουν ορισμένα είδη σφαλμάτων) τις οποίες μπορεί να μοιράζεται με τρίτα μέρη. Το Chrome OS αποθηκεύει πληροφορίες σχετικά με το ιστορικό περιήγησης τοπικά στον υπολογιστή τις οποίες ο χρήστης μπορεί να διαγράψει. Τέλος ο χρήστης με την λειτουργία Guest Mode μπορεί να χρησιμοποιήσει το Chrome OS με ένα τρόπο ώστε να μην στέλνονται προσωπικές πληροφορίες στην Google.[28]

Το «νέφος» είναι πραγματικότητα. Με πολύ γρήγορο ρυθμό οι υπηρεσίες του διευρύνονται και βρίσκουν όλο και περισσότερες εφαρμογές στην καθημερινότητά μας. Όμως τα ζητήματα ιδιωτικότητας που προκύπτουν αποτελούν μεγάλο αγκάθι σε αυτή την εξάπλωση. Μόνο όταν οι χρήστες νοιώσουν πως τα δεδομένα τους είναι ασφαλή και προστατεύεται η ιδιωτικότητα τους στον μέγιστο δυνατό βαθμό θα αξιοποιήσουν πλήρως τις δυνατότητες που το «νέφος» προσφέρει. Μια λύση για την προστασία της ιδιωτικότητας των δεδομένων των χρηστών θα μπορούσε να ήταν η μέθοδος opt-in-opt-out (π.χ. στο Facebook να υπάρχει η δυνατότητα οι χρήστες να επιλέγουν εάν θέλουν τα δεδομένα τους να χρησιμοποιηθούν σε στατιστικές έρευνες και όχι να αποτελεί προεπιλογή από τους διαχειριστές του δικτυακού τόπου). Μια άλλη λύση είναι οι ηλεκτρονικές ταυτότητες, οι οποίες δίνουν την δυνατότητα στους χρήστες να αποκαλύπτουν μόνο τα δεδομένα που είναι απαραίτητα για την

πραγματοποίηση κάποιας συναλλαγής ή την χρήση κάποιας υπηρεσίας, να λαμβάνει χώρα δηλαδή αυτό που ονομάζουμε *ελάχιστη αποκάλυψη*. Για παράδειγμα, όταν κάποιος χρήστης επιθυμεί να ενοικιάσει ένα αυτοκίνητο, στην εταιρεία ενοικίασης αρκεί να επικυρώσει το γεγονός πως ο χρήστης είναι ενήλικος και έχει δίπλωμα οδήγησης. Επιπλέον πληροφορίες όπως η ημερομηνία γέννησης του χρήστη ή ο αριθμός διπλώματος οδήγησης, δεν είναι απαραίτητο να αποκαλυφθούν. Σαφώς, σε περίπτωση που αυτό είναι απαραίτητο π.χ. σε περίπτωση ατυχήματος η αποκάλυψη περισσότερων δεδομένων των χρήστη είναι αναπόφευκτη. Τέλος, πρέπει να τονιστεί πως οι λύσεις που θα προταθούν δεν θα πρέπει να είναι μόνο τεχνολογικής φύσεως. Απαιτείται σύνθετη αντιμετώπιση με συνδυασμό τεχνολογικών επιτευγμάτων και υιοθέτηση κατάλληλου νομικού και ρυθμιστικού πλαισίου.

4 ABC4Trust

Με την εξάπλωση των εφαρμογών του νέφους μεγαλώνουν και τα προβλήματα ιδιωτικότητας. Η σημασία των προβλημάτων αυτών είναι ανάλογη της σημασίας των εφαρμογών «νέφους» για τους χρήστες. Ένα σημαντικό όπλο για την προστασία της ιδιωτικότητας αποτελούν οι νέες μορφές των ηλεκτρονικών ταυτοτήτων διότι αν δεν ληφθούν κατάλληλα μέτρα το γεγονός πως ένας χρήστης έχει όλα τα στοιχεία του σε μια κάρτα ίσως να είναι επικίνδυνο. Έχουν γίνει διάφορες προσπάθειες για να υλοποιηθεί η προσέγγιση της «ελάχιστης αποκάλυψης». Πριν λίγους μήνες άρχισε σε ερευνητικό επίπεδο το έργο ABC4Trust[16]. Πριν όμως αναφερθούμε αναλυτικότερα στο ABC4Trust θα περιγράψουμε τα *Διαπιστευτήρια που βασίζονται στα χαρακτηριστικά* (Attribute Based Credentials – ABCs).

4.1 Attribute Based Διαπιστευτήρια

Ο αριθμός των ηλεκτρονικών συναλλαγών που πραγματοποιούμε καθημερινά αυξάνεται διαρκώς. Από ηλεκτρονικό εμπόριο και e-banking μέχρι δοσοληψίες με κυβερνητικούς φορείς. Σχεδόν όλες οι εφαρμογές και οι υπηρεσίες που βασίζονται σε συστήματα ηλεκτρονικών υπολογιστών απαιτούν κάποια *αυθεντικοποίηση* (authentication) για την δημιουργία έμπιστων σχέσεων, είτε μόνο για το ένα άκρο της επικοινωνίας είτε και για τα δύο. Ορισμένες χώρες έχουν ήδη θεσπίσει ή πρόκειται να θεσπίσουν τις *ηλεκτρονικές ταυτότητες* (electronic Identity). Ηλεκτρονικά εισιτήρια και συστήματα διοδίων χρησιμοποιούνται ευρέως σε όλο τον κόσμο. Καθώς οι ηλεκτρονικές συσκευές που απαιτούν ταυτοποίηση και αυθεντικοποίηση έχουν εξαπλωθεί ευρέως σε ένα ευρύ χάσμα σεναρίων, η ιδιωτικότητα του χρήστη θα απειλείται όλο και περισσότερο στην μελλοντική κοινωνία του Διαδικτύου.

Ποια όμως είναι τα μέσα για την προστασία της ιδιωτικότητας των χρηστών; Τα ηλεκτρονικά διακριτικά ελέγχου ταυτότητας (authentication tokens)[17] καθώς και οι

[16] Περισσότερες πληροφορίες στην ηλεκτρονική διεύθυνση https://abc4trust.eu/

[17] Ένα διακριτικό ασφαλείας (security token) μπορεί να είναι μια φυσική συσκευή που δίνεται σ' έναν εξουσιοδοτημένο χρήστη για να διευκολύνει την αυθεντικοποίηση. Τα διακριτικά ασφαλείας χρησιμοποιούνται για να αποδείξουν την ηλεκτρονική ταυτότητα κάποιου (όπως στην περίπτωση ενός πελάτη που προσπαθεί να αποκτήσει πρόσβαση στον λογαριασμό τραπέζης του). Το διακριτικό χρησιμοποιείται είτε συμπληρωματικά είτε σε αντικατάσταση ενός κωδικού πρόσβασης για να

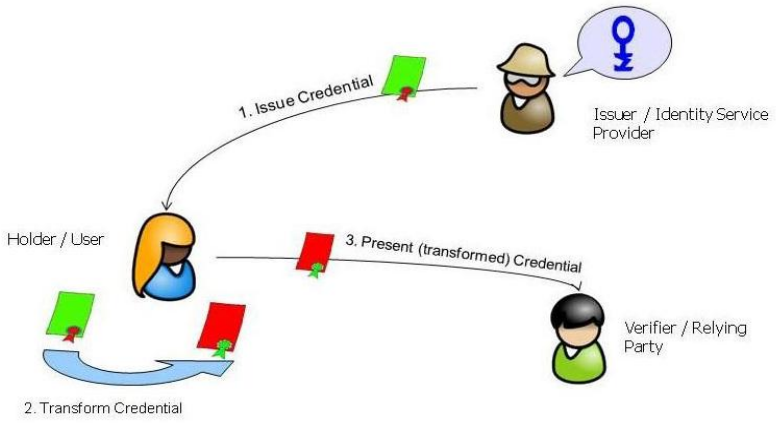
μηχανισμοί που παρέχουν είναι πολύ γνωστά επειδή δεν χρησιμοποιούνται μόνο στο Διαδίκτυο αλλά και αλλού. Πράγματι, οι παραδοσιακού τύπου ηλεκτρονικές ταυτότητες, η αυθεντικοποίηση από κινητά τηλέφωνα και τα RFID διακριτικά[18] εξαπλώνονται γρήγορα. Αυτοί οι μηχανισμοί αυθεντικοποίησης δυστυχώς έχουν την αδυναμία πως χρησιμοποιούν μοναδικά αναγνωριστικά τα οποία παρουσιάζουν τον κίνδυνο ότι μπορούν να συνδέσουν διάφορες συναλλαγές με τον ίδιο τον χρήστη, με αποτέλεσμα να απειλείται σοβαρά η ιδιωτικότητα του. Ένας άλλος διαδεδομένος μηχανισμός είναι η αυθεντικοποίηση με την χρήση κωδικών πρόσβασης που όμως παρουσιάζει πολλές αδυναμίες. Τα κρυπτογραφικά πιστοποιητικά (cryptographic certificates) παρόλο που μπορούν να προσφέρουν επαρκή ασφάλεια για αρκετούς σκοπούς, δεν καλύπτουν τις ανάγκες της ιδιωτικότητας γιατί συνδέονται μ' ένα υπαρκτό πρόσωπο. Οποιαδήποτε χρήση ενός τέτοιου πιστοποιητικού εκθέτει την ταυτότητα του κατόχου στο μέρος που ζητά την αυθεντικοποίηση. Υπάρχουν πολλά σενάρια όπου η χρήση τέτοιων πιστοποιητικών αποκαλύπτει την ταυτότητα του κατόχου χωρίς να είναι απαραίτητο, για παράδειγμα σενάρια όπου η υπηρεσία χρειάζεται μόνο να εξακριβώσει την ηλικία ενός χρήστη και όχι την πραγματική του/της ταυτότητα. Η αποκάλυψη περισσότερων πληροφοριών από τις απαραίτητες όχι μόνο ζημιώνει την ιδιωτικότητα των χρηστών αλλά αυξάνει και το ρίσκο κακής χρήσης των πληροφοριών του, όπως κλοπή ταυτότητας, όταν οι πληροφορίες πέσουν σε λάθος χέρια.

Τα κλασσικά διαπιστευτήρια λοιπόν δεν προστατεύουν την ιδιωτικότητα. Κατά κανόνα αποκαλύπτουν την ταυτότητα του κατόχου του διαπιστευτηρίου, παρόλο που συχνά η χρήση της υπηρεσίας απαιτεί λιγότερη πληροφορία, για παράδειγμα μόνο την επιβεβαίωση ότι ο κάτοχος είναι έφηβος ή δικαιούται κοινωνικές παροχές. Εν αντιθέσει, τα ABCs επιτρέπουν στον κάτοχο να αποκαλύψει μόνο την ελάχιστη πληροφορία που απαιτείται από την εφαρμογή, χωρίς να αποκαλύπτουν μια πλήρη ταυτότητα. Αυτά τα διαπιστευτήρια διευκολύνουν έτσι την υλοποίηση μιας αξιόπιστης ψηφιακής κοινωνίας που ταυτόχρονα προστατεύει την ιδιωτικότητα. Τα τελευταία 25 χρόνια έχουν αναπτυχθεί μια σειρά από τεχνολογίες για την κατασκευή ABC συστημάτων με έναν τρόπο ώστε να είναι έμπιστα, όπως τα κρυπτογραφικά

αποδείξει πως ο πελάτης είναι πραγματικά αυτός που ισχυρίζεται. Το διακριτικό λειτουργεί σαν ένα ηλεκτρονικό κλειδί για να έχουμε πρόσβαση σε κάτι.

[18] Το RFID είναι ένα σύστημα ασύρματης αναγνώρισης αντικειμένων και ήρθε να αντικαταστήσει το Bar Code.

πιστοποιητικά, ενώ ταυτόχρονα να προστατεύουν την ιδιωτικότητα του κατόχου τους. Τέτοια ABCs εκδίδονται όπως τα κρυπτογραφικά διαπιστευτήρια (π.χ. τα X.509 διαπιστευτήρια) χρησιμοποιώντας ένα ψηφιακό (μυστικό) κλειδί υπογραφής (signature key). Ένα ABC επιτρέπει στον κάτοχό του να το μετατρέψει σ' ένα νέο διαπιστευτήριο που περιέχει μόνο ένα υποσύνολο των *χαρακτηριστικών* (attributes) που περιέχονται στο αρχικό διαπιστευτήριο. Αυτά τα διαπιστευτήρια μπορούν να επαληθευτούν όπως τα κοινά κρυπτογραφικά διαπιστευτήρια (χρησιμοποιώντας το δημόσιο κλειδί επαλήθευσης του εκδότη) και προσφέρουν την ίδια ασφάλεια (βλέπε Εικόνα 3 παρακάτω). Οι τεχνολογίες ABC, που συχνά ονομάζονται στην βιβλιογραφία *ανώνυμα συστήματα διαπιστευτηρίων*, επιτρέπουν σ' έναν πάροχο υπηρεσιών ταυτότητας (identity service provider) να εκδώσει ένα διαπιστευτήριο (ή πιστοποιητικό) σ' έναν χρήστη. Αυτό το διαπιστευτήριο περιέχει χαρακτηριστικά του χρήστη όπως διεύθυνση ή ημερομηνία γέννησης αλλά και τα δικαιώματα του χρήστη ή ρόλους του ως χαρακτηριστικά. Χρησιμοποιώντας το διαπιστευτήριο, ο χρήστης μπορεί να αποδείξει σ' ένα τρίτο μέρος ότι έχει στην κατοχή του ένα διαπιστευτήριο που περιέχει ένα συγκεκριμένο χαρακτηριστικό ή ρόλο χωρίς να αποκαλύπτει άλλες πληροφορίες που είναι αποθηκευμένες στο διαπιστευτήριο. Για παράδειγμα, ο χρήστης μπορεί να χρησιμοποιήσει ένα ανώνυμο ID διαπιστευτήριο που έχει εκδοθεί από την κυβέρνηση για να αποδείξει πως είναι ενήλικας, δηλαδή πως έχει ένα διαπιστευτήριο που περιέχει μια ημερομηνία γέννησης που είναι μεγαλύτερη από 18 χρόνια πριν. Ως εκ τούτου, τα ανώνυμα διαπιστευτήρια (anonymous credentials) υπόσχονται να είναι ο ακρογωνιαίος λίθος για την προστασία της ιδιωτικότητας του χρήστη σ' ένα ηλεκτρονικό περιβάλλον.



Εικόνα 3. Επαλήθευση ενός attribute-based διαπιστευτηρίου

4.2 Περιγραφή του έργου ABC4Trust

Όπως έχει ήδη αναφερθεί, σχεδόν όλες οι εφαρμογές και οι υπηρεσίες που βασίζονται σε συστήματα ηλεκτρονικών υπολογιστών απαιτούν κάποια αυθεντικοποίηση για την δημιουργία έμπιστων σχέσεων. Παρόλα αυτά, τα παραδοσιακά διαπιστευτήρια δεν προστατεύουν την ιδιωτικότητα του χρήστη. Η λύση φαίνεται πως είναι τα ABCs.

Υπάρχουν στην βιβλιογραφία πολλές προτάσεις για το πώς μπορεί να υλοποιηθεί ένα ABC σύστημα. Αξιοσημείωτη είναι η εμφάνιση δυο τεχνολογιών, η Identity Mixer της IBM και η U-Prove της Microsoft.

Η τεχνολογία Identity Mixer είναι ένα ανώνυμο σύστημα διαπιστευτηρίων που αναπτύχθηκε από την IBM Research το οποίο παρέχει ισχυρή αυθεντικοποίηση και ιδιωτικότητα ταυτόχρονα. Με την Identity Mixer οι χρήστες μπορούν να προμηθευτούν από τον εκδότη ένα διαπιστευτήριο που να περιέχει όλες τις πληροφορίες που ο εκδότης μπορεί να πιστοποιήσει γι' αυτούς. Όταν αργότερα ένας χρήστης θέλει να αποδείξει σ' έναν πάροχο υπηρεσιών έναν ισχυρισμό (claim) για τον ίδιο, χρησιμοποιεί την Identity Mixer για να μετασχηματίσει με ασφάλεια το εκδοθέν διαπιστευτήριο. Το μετασχηματισμένο διαπιστευτήριο θα περιέχει μόνο ένα υποσύνολο των πιστοποιημένων πληροφοριών που ο χρήστης είναι πρόθυμος να αποκαλύψει. Ο χρήστης μπορεί να πραγματοποιήσει αυτόν το μετασχηματισμό όσες φορές θελήσει χωρίς τα διαπιστευτήρια να μπορούν να διασυνδεθούν μεταξύ τους. [29]

Η U-Prove είναι μια προηγμένη τεχνολογία κρυπτογράφησης, η οποία σε συνδυασμό με τις υπάρχουσες λύσεις ταυτοποίησης που βασίζονται σε πρότυπα, ξεπερνά το μακροχρόνιο δίλημμα ανάμεσα στην διασφάλιση της ταυτότητας και στην ιδιωτικότητα. Αυτό επιτρέπει την υλοποίηση πολλών σεναρίων που στο παρελθόν δεν μπορούσαν να πραγματοποιηθούν και απαιτούσαν επαληθευμένα στοιχεία ταυτότητας και ιδιωτικότητα. [30]

Δεδομένου ότι αυτές οι τεχνολογίες υποστηρίζονται από τις δύο κορυφαίες εταιρείες στον χώρο, είναι μεταξύ των καλύτερων υποψηφίων για να συνεισφέρουν στην διαδικασία τυποποίησης σε αυτόν τον τομέα. Ωστόσο η πολυπλοκότητα των ABC τεχνολογιών και οι αλληλεπιδράσεις client-server που συνεπάγονται, έχουν μέχρι τώρα αποθαρρύνει πιθανούς χρήστες και κατά συνέπεια παρεμποδίζουν την ανάπτυξή

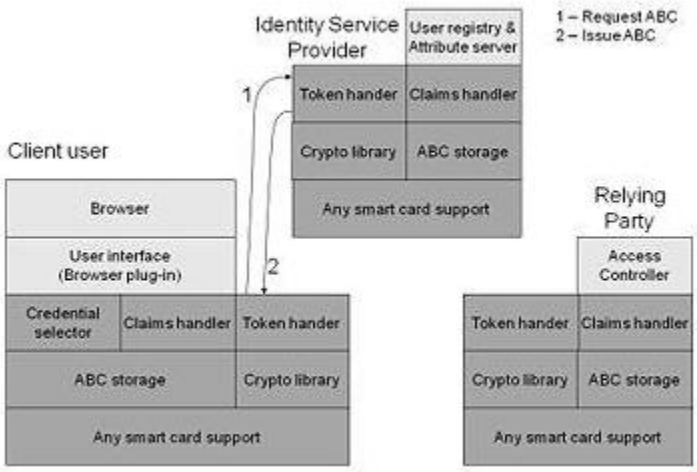
τους σε μεγάλη κλίμακα. Το να ξεπεραστούν αυτά τα εμπόδια απαιτεί μία εις βάθος συγκριτική μελέτη των λειτουργιών των διαφορετικών ABC τεχνολογιών και ανάλυση της ασφάλειάς και της αποδοτικότητάς τους ώστε να προκύψει μια κοινή αντίληψη για την εφαρμογή τους σε ποικίλα πεδία εφαρμογής και σενάρια.

Με μια συγκριτική αντίληψη αυτών των τεχνολογιών, θα είναι ευκολότερο για διαφορετικές κοινότητες χρηστών να αποφασίσουν σε ένα συγκεκριμένο σενάριο εφαρμογής ποια τεχνολογία τους εξυπηρετεί καλύτερα. Θα είναι επίσης ευκολότερο να μεταβούν σε νεότερες ABC τεχνολογίες που σίγουρα θα προκύψουν με την πάροδο του χρόνου. Επιπλέον οι ίδιοι οι χρήστες μπορεί να θέλουν να έχουν πρόσβαση σε εφαρμογές που απαιτούν διαφορετικές ABC τεχνολογίες, και οι ίδιες οι εφαρμογές μπορεί να θέλουν να καλύψουν τις ανάγκες κοινοτήτων χρηστών που προτιμούν διαφορετικές ABC τεχνολογίες. Ως εκ τούτου είναι απαραίτητο διαφορετικές ABC τεχνολογίες να μπορούν να συνυπάρχουν ή να εναλλάσσονται σε σενάρια που αφορούν τους ίδιους χρήστες και πλατφόρμες εφαρμογών. Δεν υπάρχουν κοινώς συμφωνημένα σύνολα λειτουργιών και χαρακτηριστικά για την μέτρηση και σύγκριση των ABC τεχνολογιών, έτσι είναι δύσκολο να κρίνουμε τα αντίστοιχα πλεονεκτήματα και μειονεκτήματα τους. Δεν υπάρχει επίσης προς το παρόν καθιερωμένη πρακτική ή πρότυπα που να επιτρέπουν την εναλλαξιμότητα και την ενοποίηση των ABC τεχνολογιών.

Στόχος του έργου ABC4Trust είναι η κατανόηση εις βάθος των ABC τεχνολογιών, η αποδοτική και αποτελεσματική ανάπτυξή τους στην πράξη, και η ενοποίηση τους σε διαφορετικούς τομείς. Για τον σκοπό αυτό το έργο θα:

- Δημιουργήσει ένα αρχιτεκτονικό πλαίσιο για τις ABC τεχνολογίες που θα επιτρέπει σε διαφορετικές πραγματοποιήσεις αυτών των τεχνολογιών να συνυπάρχουν, να εναλλάσσονται και να ενοποιούνται, δηλαδή θα
    - Αναγνωρίσει και περιγράψει διαφορετικές λειτουργικές συνιστώσες των ABC τεχνολογιών π.χ. για αίτηση και έκδοση των διαπιστευτηρίων (βλέπε εικόνα 4)
    - Δημιουργήσει προδιαγραφές για τις μορφές δεδομένων, διεπαφές και μορφές πρωτόκολλων γι’ αυτό το πλαίσιο
- Ορίσει κριτήρια για την σύγκριση των ιδιοτήτων των πραγματοποιήσεων αυτών των συνιστωσών στις διαφορετικές τεχνολογίες

- Παρέχει σχετικές υλοποιήσεις για κάθε μια από αυτές τις συνιστώσες



Εικόνα 4. Αίτηση και έκδοση διαπιστευτηρίων

Αυτά τα τρία αποτελέσματα θα επιτρέψουν στα ενδιαφερόμενα μέρη να κατανοήσουν καλύτερα τις ABC τεχνολογίες, να συγκρίνουν τα πλεονεκτήματα των διαφόρων τεχνολογιών σε διαφορετικά σενάρια, να αξιοποιήσουν πλήρως τα χαρακτηριστικά τους τα οποία ενισχύουν την ιδιωτικότητα, και έτσι να αναπτύξουν αποτελεσματικά αυτές τις τεχνολογίες με την πεποίθηση πως υπάρχει ένας δρόμος προς την εξέλιξη και την αντικατάστασή τους με την πάροδο του χρόνου.

4.2.1 Στόχοι του έργου

Το έργο έχει έξι στόχους οι οποίοι περιγράφονται παρακάτω: [31]

1. Να προτείνει ένα πλαίσιο για τις αρχιτεκτονικές διεπαφές που είναι ανεξάρτητες τεχνολογίας, για τα πρωτόκολλα και για την λειτουργία των ABC τεχνολογιών, έτσι ώστε διαφορετικές τεχνολογίες να μπορούν να συνυπάρξουν για να ανταποκριθούν στις διαφορετικές απαιτήσεις των εφαρμογών, να εναλλάσσονται και να ενοποιούνται καθώς οι τεχνολογίες αυτές εξελίσσονται

2. Να αναλύσει και να συγκρίνει τις αναδυόμενες ABC τεχνολογίες σε σχέση με τα χαρακτηριστικά τους, την ροή πληροφοριών, την ασφάλεια, την επίδοση και άλλα πλεονεκτήματα και μειονεκτήματα σε διάφορα σενάρια εφαρμογής
3. Να αναπτύξει σχετικές υλοποιήσεις αυτών των τεχνολογιών που να μπορούν να μεταφερθούν σε διαφορετικές πλατφόρμες ή συνδυασμούς πλατφορμών
4. Να προσδιορίσει τις απαιτήσεις εφαρμογών και επιχειρήσεων για την ετοιμασία πιλοτικών εφαρμογών για κάποιες από αυτές τις τεχνολογίες
5. Να αναπτύξει πιλοτικές εφαρμογές για τον έλεγχο αξιοπιστίας της παραπάνω αρχιτεκτονικής πρότασης, να εξερευνήσει τις ABC αρχιτεκτονικές στην πράξη, και να αξιολογήσει την χρηστικότητά τους σε πραγματικά σενάρια εφαρμογών και επιχειρήσεων
6. Να αποτελέσει τον κινητήριο μοχλό ώστε οι κορυφαίες εταιρείες που συμπεριλαμβάνονται στο έργο να στοχεύσουν στην τυποποίηση, και να γίνουν ευρέως γνωστά τα αποτελέσματα του έργου, εκτός των άλλων εκδίδοντας ένα βιβλίο που θα δίνει την δυνατότητα στο ευρύ κοινό να έχει πρόσβαση στην γνώση για την ABC τεχνολογία και τις πιλοτικές εφαρμογές.

Το έργο περιλαμβάνει δύο πιλοτικές εφαρμογές: [31]

1. Η πρώτη πιλοτική εφαρμογή που πραγματοποιείται σ’ ένα σχολείο της Σουηδίας, θα περιλαμβάνει πρόσβαση στην κοινότητα του σχολείου με την χρήση ψευδώνυμων και κοινωνική δικτύωση για τους μαθητές του σχολείου. Συγκεκριμένα, οι μαθητές θα μπορούν να ζητούν συμβουλές και να κάνουν πολύ προσωπικές ερωτήσεις που αφορούν την φυσική, ψυχολογική, κοινωνική, οικονομική κλπ. κατάστασή τους, από γιατρούς, νοσοκόμες, ψυχολόγους κλπ. χωρίς κατ’ ανάγκη να αποκαλύπτουν την πραγματική τους ταυτότητα. Αυτή η πιλοτική εφαρμογή θα αντιμετωπίσει τις ειδικές προκλήσεις που τίθενται από το γεγονός ότι οι χρήστες του Διαδικτύου είναι όλο και μικρότερης ηλικίας και μερικές φορές είναι ανήλικοι. Σήμερα τα σχολεία στην Σουηδία χρησιμοποιούν το Διαδίκτυο κυρίως για την επικοινωνία ανάμεσα σε μαθητές, καθηγητές και γονείς. Χρησιμοποιούν διαφορετικές πύλες και ιδιωτικές κοινότητες για να πραγματοποιήσουν αυτήν την επικοινωνία. Μια μεγάλη απειλή για την ιδιωτικότητα των μαθητών είναι η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες,

όπως βαθμοί και αποτελέσματα διαγωνισμάτων των μαθητών, αλλά και άλλες πληροφορίες και λειτουργίες που είναι διαθέσιμες μέσω της πύλης του σχολείου. Πολλές εφαρμογές, όπως η κοινωνική δικτύωση και παροχή ιατρικών συμβουλών θα επωφεληθούν από το έργο ABC4Trust, καθώς επιτρέπει τον συνδυασμό ισχυρής αυθεντικοποίησης και προστασία της ιδιωτικότητας σε μία μόνο λύση. Η προτεινόμενη κοινότητα θα προστατεύσει την ταυτότητα των μαθητών ενάντια στην κλοπή πληροφοριών, όπως επίσης θα προστατεύσει και την ιδιωτικότητα τους. Από την μια μεριά, οι μαθητές θα μπορούν να βεβαιώνουν την ταυτότητά τους για να έχουν πρόσβαση σε chat rooms και εμπιστευτικές πληροφορίες. Από την άλλη πλευρά, θα μπορούν να μένουν ανώνυμοι όταν ερωτούνται προσωπικές και ευαίσθητες πληροφορίες από το προσωπικό του σχολείου, ενώ παράλληλα το προσωπικό του σχολείου θα διασφαλίζει πως επικοινωνεί με εξουσιοδοτημένους μαθητές του αντίστοιχου σχολείου ή τάξης. Η πιλοτική εφαρμογή θα βοηθήσει ώστε να συγκεντρωθούν πληροφορίες για την χρηστικότητα του προτεινόμενου ABC συστήματος κάτω από ιδιαίτερα δύσκολες συνθήκες χρήσης του, μιας και οι χρήστες του θα είναι παιδιά.

2. Η δεύτερη πιλοτική εφαρμογή θα πραγματοποιηθεί στην Ελλάδα στο Πανεπιστήμιο Πατρών, και θα περιλαμβάνει δημοσκόπηση, και ειδικότερα ανώνυμη συλλογή ανατροφοδότησης από εξουσιοδοτημένους φοιτητές σχετικά με τα μαθήματα που παρακολούθησαν και τους καθηγητές που τους δίδαξαν τα μαθήματα αυτά. Σε αυτή την περίπτωση θα εκδοθούν διαπιστευτήρια σε φοιτητές που θα πιστοποιούν μια σειρά από γεγονότα για αυτούς (έτος σπουδών, ποσοστό φυσικής παρουσίας σ' ένα μάθημα κλπ.), επιτρέποντας σε φοιτητές με τα κατάλληλα διαπιστευτήρια να παρέχουν ανώνυμα ανατροφοδότηση για τα μαθήματα και τους καθηγητές που είχαν κατά την διάρκεια του διδακτικού εξαμήνου ή έτους. Για να μπορεί κάποιος φοιτητής να συμμετάσχει, θα πρέπει τα διαπιστευτήριά του να αποδεικνύουν κάποια γεγονότα γι' αυτόν, δηλαδή αν έχει επιλέξει το μάθημα, το έτος εγγραφής του στο πανεπιστήμιο, και την αναλογία φυσικής παρουσίας του στην τάξη. Το γεγονός εάν η φυσική παρουσία του στην τάξη είναι επαρκής δεν θα αποδειχτεί αποκαλύπτοντας το ακριβές ποσοστό παρουσιών (καθώς αυτό μπορεί να χρησιμοποιηθεί για να αποκαλυφθεί ο φοιτητής), αλλά δείχνοντας ότι είναι πάνω από το προκαθορισμένο όριο που επιτρέπει στον

φοιτητή να λάβει μέρος στην αξιολόγηση. Αυτή η πιλοτική εφαρμογή θα αντιμετωπίσει την ιδιαίτερη πρόκληση ότι για να είναι τα αποτελέσματα μιας δημοσκόπησης ορθά και αξιόπιστα θα πρέπει να διατηρείται η ιδιωτικότητα των ατόμων που εκφράζουν την γνώμη τους. Η αξιολόγηση μαθημάτων έχει γίνει συνήθη πρακτική στα περισσότερα πανεπιστήμια του σύγχρονου βιομηχανικού κόσμου. Παρόλα αυτά, συνήθως πραγματοποιούνται εκτός ηλεκτρονικού υπολογιστή για να προστατευτεί η ιδιωτικότητα των φοιτητών. Εάν διεξάγονταν μέσω υπολογιστών, οι υπολογιστές θα έπρεπε να λειτουργούν κάτω από το πρίσμα ενός ουδέτερου αξιόπιστου οργανισμού, ανεξάρτητου από το πανεπιστήμιο που κάνει την αξιολόγηση, διαφορετικά οι φοιτητές θα έπρεπε να είχαν τεράστια εμπιστοσύνη στις πρακτικές προστασίας της ιδιωτικότητας που εφαρμόζει το εκάστοτε πανεπιστήμιο. Οι ABC τεχνολογίες θα επιτρέπουν σε κάθε πανεπιστήμιο να εκδίδει τα δικά του ηλεκτρονικά φοιτητικά δελτία ταυτότητας τα οποία θα περιέχουν λίστες με τα μαθήματα που κάθε φοιτητής δήλωσε. Στην συνέχεια, το πανεπιστήμιο θα μπορεί να τρέχει το δικό του ηλεκτρονικό σύστημα ανατροφοδότησης χωρίς να χρειάζεται να αποκτήσει την εμπιστοσύνη των φοιτητών, γιατί οι ABC τεχνολογίες χρησιμοποιούμενες στα δελτία ταυτότητας θα αποκόπτουν όλους τους συνδέσμους ανάμεσα στην εισερχόμενη ηλεκτρονική ανατροφοδότηση και την ταυτότητα του φοιτητή που την υπέβαλλε, εξασφαλίζοντας παράλληλα πως η ανατροφοδότηση προέρχεται από διαπιστευμένους φοιτητές. Η πιλοτική εφαρμογή θα βοηθήσει ώστε να συγκεντρωθούν πληροφορίες για τις αντιδράσεις μιας κατεξοχήν κρίσιμης ομάδας χρηστών.

4.2.2 Εξελίξεις πέρα από την τελευταία λέξη της τεχνολογίας

Το ABC4Trust θα μπορούσε να συμβάλλει στην εξέλιξη της τελευταίας λέξης της τεχνολογίας τουλάχιστον σε επτά περιοχές: [31]

1. **Ένα πλαίσιο για την ενοποίηση και εναλλαξιμότητα των ABC συστημάτων**

Υπάρχει πλήθος προτύπων και αρχιτεκτονικών που επιτρέπουν την ενοποίηση και εναλλαξιμότητα των συστημάτων και μηχανισμών ταυτοποίησης. Π.χ. Liberty

Alliance, OpenID, OASIS Information Cards κλπ. Ωστόσο τέτοια ενιαία πρότυπα και αρχιτεκτονικές δεν υπάρχουν για τα ABC συστήματα. Μια πρώτη συμβολή αυτού του έργου στην εξέλιξη της τεχνολογίας θα είναι ο ορισμός μιας τέτοιας κοινής ενοποιημένης αρχιτεκτονικής για την ενοποίηση και εναλλαξιμότητα διαφορετικών ABC συστημάτων έτσι ώστε:

- Οι χρήστες να μπορούν να αποκτούν διαπιστευτήρια για πολλές ABC τεχνολογίες και να τα χρησιμοποιούν με διαφορετικό τρόπο στις ίδιες πλατφόρμες υλικού και λογισμικού
- Οι πάροχοι υπηρεσιών να μπορούν να υιοθετούν οποιαδήποτε ABC τεχνολογία ταιριάζει καλύτερα με τις ανάγκες τους
- Οι πάροχοι υπηρεσιών ταυτοποίησης (identity service providers) να είναι σε θέση να δέχονται διαπιστευτήρια μιας συγκεκριμένης ABC τεχνολογίας και να εκδίδουν αντίστοιχα διαπιστευτήρια μιας άλλης ABC τεχνολογίας, χρησιμοποιώντας και πάλι τις ίδιες πλατφόρμες υλικού και λογισμικού.

2. Ακριβείς και πλήρεις μετρικές για την σύγκριση υπαρχόντων ABC συστημάτων

Τα διαπιστευτήρια που βασίζονται στην ταυτότητα (Identity Based Credentials) υπάρχουν εδώ και πολλά χρόνια και υπάρχουν πολλά παραδείγματα και υλοποιήσεις αυτών των τεχνολογιών (X509, EMV, DANID, ESTID). Τα ABCs που επιτρέπουν στους χρήστες να αποδεικνύουν ιδιότητες ή χαρακτηριστικά για τους ίδιους χωρίς να αποκαλύπτουν την ακριβή τους ταυτότητα, είναι μια πιο πρόσφατη ιδέα. Μόνο οι τεχνολογίες Identity Mixer της IBM και U-Prove της Microsoft έχουν προταθεί έως τώρα.

Δεν υπάρχει σχεδόν καθόλου εμπειρία για την υλοποίηση τους, την ανάπτυξή, και την χρήση τους στην πράξη. Στην πραγματικότητα, αυτές οι τεχνολογίες βρίσκονται σε διαφορετικά στάδια ωρίμανσης και προσφέρουν διαφορετικές δυνατότητες για επεκτάσεις και γενικεύσεις. Για παράδειγμα, η Identity Mixer είναι στην πραγματικότητα μια οικογένεια πρωτοκόλλων, ενώ η U-Prove είναι μια προδιαγραφή του πυρήνα λειτουργικότητας ενός ευρύτερου συνόλου πρωτοκόλλων. Δεν υπάρχει λοιπόν ένας συστηματικός τρόπος για να αναλυθούν και να συγκριθούν αυτές οι

τεχνολογίες. Το έργο ABC4Trust θα προσφέρει ένα πλαίσιο για να πραγματοποιηθεί αυτό με αυστηρότητα.

Το έργο θα συμβάλλει στην εξέλιξη της τεχνολογίας, παρέχοντας ένα πλαίσιο με μετρικές για την σύγκριση διαφορετικών ABC συστημάτων κατά μήκος τεσσάρων διαστάσεων: λειτουργική κάλυψη, ιδιότητες ασφάλειας, απόδοση και αναγκαία υποστήριξη υλικού για λόγους απόδοσης ή ασφάλειας, και συγκεκριμένα:

- Μια συστηματική και λειτουργική επισκόπηση και σύγκριση των ιδιοτήτων των διαφόρων ABC συστημάτων – υπάρχουν μόνο ad-hoc[19] επισκοπήσεις οι οποίες δεν παρέχουν μια σταθερή βάση για την σύγκριση των λειτουργικών ιδιοτήτων
- Μια συστηματική σύγκριση της σχετικής απόδοσης που μπορεί κάποιος να περιμένει για διαφορετικά ABC συστήματα
- Μια συστηματική ανάλυση του τι είδους υποστήριξη υλικού χρειάζεται ή μπορεί να υποστηρίξει κάθε ABC σύστημα, για σκοπούς αυξημένης ασφάλειας ή απόδοσης
- Μετρικές για την αξιολόγηση των ABC συστημάτων κατά μήκος των παραπάνω διαστάσεων λειτουργίας, ασφάλειας, επίδοσης και υποστήριξης υλικού.

3. Μια σχετική υλοποίηση για επιλεγμένα ABC συστήματα

Το έργο θα παρέχει σχετική υλοποίηση για τις συνιστώσες που ορίζουν ένα ABC σύστημα και για κάποιες από τις συνιστώσες θα υλοποιηθούν περισσότεροι κρυπτογραφικοί αλγόριθμοι. Αυτή η διαδικασία θα δείξει την έκταση στην οποία διαφορετικές προτάσεις για ABC συστήματα μπορούν να είναι διαλειτουργικές και είναι κρίσιμη για την επίτευξη του στόχου του έργου.

Υπάρχουν ήδη υλοποιήσεις των ABC συστημάτων για τα συστήματα Identity Mixer της IBM και U-Prove της Microsoft. Παρόλα αυτά, αυτές οι υλοποιήσεις ακολουθούν διαφορετικές αρχιτεκτονικές. Δεν υπάρχουν κοινώς συμφωνημένα σύνολα λειτουργιών, χαρακτηριστικών και πρωτοκόλλων που θα επιτρέπουν την ενοποίηση ή

[19] Δηλώνει γενικά μια λύση σχεδιασμένη για ένα συγκεκριμένο πρόβλημα, μη γενικευμένη, η οποία δεν προορίζεται να μπορεί να προσαρμοστεί για άλλους σκοπούς

την διαλειτουργικότητα, πόσο μάλλον την συνεργασία σ' ένα κοινό σενάριο. Μια σχετική υλοποίηση σύμφωνη με το αρχιτεκτονικό πλαίσιο θα προσφέρει τέτοιες βελτιώσεις. Θα μπορεί ακόμα να επιτρέψει την αποθήκευση και διαχείριση των διαπιστευτηρίων για κάθε σύστημα σ' έναν κοινό χώρο αποθήκευσης, ενδεχομένως σε έξυπνες κάρτες.

4. Απόκτηση εμπειρίας από τις πιλοτικές εφαρμογές

Η κοινοπραξία του έργου θα πραγματοποιήσει την πρώτη υλοποίηση των ABC συστημάτων σε περιβάλλοντα παραγωγής. Έτσι θα είναι η πρώτη φορά που η έρευνα σχετικά με την λειτουργία, την διαλειτουργικότητα, την αποδοχή των χρηστών και ούτω κάθε εξής μπορεί να διεξαχθεί σε πραγματικό περιβάλλον. Το ABC4Trust θα συγκεντρώσει αυτή την εμπειρία από δύο συγκεκριμένα περιβάλλοντα. Έχοντας αυτές τις δύο πιλοτικές εφαρμογές μπορεί να ελεγθεί η χρήση και η απόδοση των διαπιστευτηρίων με δύο ομάδες χρηστών διαφορετικών δεξιοτήτων και αναγκών. Η μια ομάδα χρηστών θα είναι παιδιά σ' ένα σχολικό περιβάλλον, ενώ το άλλο θα είναι φοιτητές σ' ένα πανεπιστήμιο. Οι περιπτώσεις χρήσης στις οποίες το έργο στοχεύει είναι αρκετά διαφορετικές, έτσι ώστε να καλύψουν ένα ευρύ χάσμα απαιτήσεων, και συνεπώς διαπιστευτηρίων.

Επιπλέον, η κατεύθυνση της ανταλλαγής πληροφοριών διαφέρει σε σχέση με τίνος η ιδιωτικότητα προστατεύεται (ο πάροχος των πληροφοριών στην Ελλάδα και ο αιτών της πληροφορίας ή συμβουλής στην Σουηδία), όπως επίσης και η δομή της ανταλλαγής πληροφοριών. Υπό αυτή την έννοια, οι δυο μελέτες είναι συμπληρωματικές και θα προσφέρουν ανατροφοδότηση μοναδικής αξίας στους προγραμματιστές της σχετικής υλοποίησης και είναι συνεπώς απαραίτητες ως πραγματικό περιβάλλον έρευνας του έργου.

Λαμβάνοντας υπόψη την συλλογή κριτηρίων και την σχεδίαση/υλοποίηση της απαραίτητης υποδομής (πάροχος υπηρεσιών ταυτότητας, υποδομή για την έκδοση των διαπιστευτηρίων π.χ. βασισμένα σε έξυπνες κάρτες, βάσεις δεδομένων χαρακτηριστικών), η αξιολόγηση των πιλοτικών εφαρμογών θα παρέχει μια σαφής απόδειξη για την δυνατότητα εφαρμογής τόσο της ιδέας των ενοποιημένων

ανώνυμων διαπιστευτηρίων όσο και για την σχετική αρχιτεκτονική, παρέχοντας παράλληλα ανατροφοδότηση για περαιτέρω βελτιώσεις.

5. Συνεισφορά στην Ευρωπαϊκή Υποδομή Διαχείρισης Ηλεκτρονικών Ταυτοτήτων (European Electronic Identity Management Infrastructure)

Η Ευρώπη στοχεύει σε μια υποδομή διαχείρισης ηλεκτρονικών ταυτοτήτων, ως βάση για αξιόπιστες υπηρεσίες στην η-διακυβέρνηση και στο η-εμπόριο ώστε να εξαλειφθούν οι κλειστές λύσεις, και η έλλειψη διαφάνειας και ελέγχου από τον χρήστη. Την ίδια στιγμή, η δημοσίευση της ENISA[20] σχετικά με «Τα χαρακτηριστικά ιδιωτικότητας των προδιαγραφών των ευρωπαϊκών ηλεκτρονικών ταυτοτήτων (eID)» (Privacy Features of European eID Card Specifications) [32] τονίζει την ανάγκη για "*χρήση μοναδικών αναγνωριστικών ώστε να σέβονται την ιδιωτικότητα*" στις αναδυόμενες ευρωπαϊκές ηλεκτρονικές ταυτότητες, και αναφέρει ρητά πως οι ABC τεχνολογίες έχουν σημαντικές δυνατότητες σε αυτό τον χώρο. Το έργο ABC4Trust μπορεί να συνεισφέρει σημαντικά για τον σχεδιασμό της επικείμενης υποδομής διαχείρισης ηλεκτρονικών καρτών με:

- Μια αντίληψη των ABC τεχνολογιών που να είναι ανεξάρτητη πρωτοκόλλων, γεφυρώνοντας έτσι το χάσμα ανάμεσα στο επίπεδο αρχιτεκτονικού πλαισίου και το επίπεδο κρυπτογράφησης, το οποίο επιβραδύνει την υιοθέτηση των ABC συστημάτων
- Πληροφορίες για την ενοποίηση των ABC συστημάτων ώστε να αποφευχθεί η εξάρτηση από μια μόνο ABC τεχνολογία, που θα είχε ως αποτέλεσμα μια μονοπωλιακή κατάσταση που δεν θα ήταν αποδεκτή για μια υποδομή.

6. Ενημέρωση των ηγετών της τεχνολογίας

Το ABC4Trust θα ενημερώνει τακτικά τους προγραμματιστές εφαρμογών και τους προμηθευτές τεχνολογίας για την πρόοδο του έργου ώστε να μπορούν να χρησιμοποιηθούν τα ABC συστήματα.

---

[20]Η ENISA (European Network and Information Security Agency - Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών) είναι ένας οργανισμός της Ευρωπαϊκής ένωσης που έχει ως στόχο να βελτιωθεί η ασφάλεια δικτύων και πληροφοριών στην Ευρωπαϊκή ένωση

Το ABC4Trust θα συνεργαστεί με επιλεγμένους φορείς τυποποίησης που ασχολούνται με ABCs και επίσης θα έρθει σε επαφή με συγκεκριμένες ομάδες εργασίας, μεταξύ άλλων ομάδες που σχετίζονται με την ηλεκτρονική διακυβέρνηση, ώστε να τους ενθαρρύνει να ενσωματώσουν τα ABCs. Τα αποτελέσματα του έργου θα κοινοποιηθούν στους ενδιαφερόμενους. Η Στρατηγική Διάχυσης θα λάβει υπόψη της διαφορετικές ομάδες στόχους και τις ανάγκες τους. Θα περιέχει τρόπους για την μετάδοση των αποτελεσμάτων του έργου καθώς και ένα σχεδιασμό για συνεργασία με εξωτερικούς φορείς. Το έργο θα παρέχει υλικό δημοσίων σχέσεων για συγκεκριμένο κοινό, ώστε να γνωρίσουν τις δυνατότητες των ABCs, και να κατανοήσουν καλύτερα πως λειτουργούν και πως μπορούν να γίνουν μέρος των σημερινών και μελλοντικών εφαρμογών. Τα αποτελέσματα του έργου θα συνοψισθούν σ' ένα βιβλίο, που θα απευθύνεται κυρίως σε προγραμματιστές εφαρμογών, ερευνητές, προμηθευτές και φορείς χάραξης πολιτικής που ανήκουν στον χώρο των Τεχνολογιών Πληροφορικής και Επικοινωνιών.

7. Αντιμετώπιση νομικών ζητημάτων

Μια κοινή πρακτική των νομικών και των δικηγόρων διαφόρων εταιρειών είναι η συλλογή σχετικών πληροφοριών για την άσκηση αστικής αγωγής ή ποινικής δίωξης. Η ανάπτυξη εργαλείων διαχείρισης ταυτοτήτων, και πόσο μάλλον των ABC τεχνολογιών, παρεμποδίζεται από τέτοιες νομικές πρακτικές. Η συλλογή και αναγνώριση τέτοιων εμποδίων σε διαφορετικούς νομικούς τομείς στους νόμους της Ευρωπαϊκής Ένωσης και ορισμένους εθνικούς νόμους είναι απαραίτητη προϋπόθεση για την επιτυχή ανάπτυξη των ABC τεχνολογιών. Η διαμόρφωση απαραίτητων νομικών προϋποθέσεων για τις ABC τεχνολογίες και η εκτίμηση του πώς οι ABC τεχνολογίες μπορούν να λύσουν αυτά τα πρακτικά και νομικά ζητήματα θα επιφέρει εξελίξεις όσο αφορά την νομική έρευνα π.χ. επιτρέποντας online ανώνυμες συναλλαγές παρέχοντας παράλληλα μια μέθοδο για να απαιτήσει ο χρήστης αξιώσεις για την άσκηση αστικής αγωγής. Το ερώτημα που το έργο ABC4Trust πρέπει να απαντήσει είναι εάν αυτό περιλαμβάνει κατά ανάγκην έναν γρήγορο, έμπιστο και αξιόπιστο τρόπο για ανάκληση της ανωνυμίας, όπως θα μπορούσε να παρέχεται από τα ABCs, και αν ναι κάτω από ποιες συνθήκες η ανωνυμία μπορεί να ανακληθεί για την άσκηση πολιτικής αγωγής. Οι προσφερόμενες λύσεις θα μπορούσαν να

περιλαμβάνουν υποδείξεις για την Ευρωπαϊκή Ένωση ή την διεθνή νομοθεσία όσο αφορά την ενσωμάτωση των ABCs στις Ευρωπαϊκές ηλεκτρονικές ταυτότητες, καθορίζοντας την αποδεικτική αξία των διαπιστευτηρίων σε αστικές δίκες ή κανονισμούς και αποφασίζοντας ποιο δικαστήριο ή όργανο είναι αρμόδιο να αποφασίζει για τις προϋποθέσεις που θα πρέπει να ισχύουν για να γίνει ανάκληση της ανωνυμίας, όταν ο τόπος διαμονής είναι άγνωστος.

Η ενσωμάτωση των νομικών σε τεχνικά πακέτα εργασίας σε μια μορφή οριζόντιας δραστηριότητας θα εξασφαλίσει πως οι νομικές απαιτήσεις θα είναι γνωστές στους ερευνητές σε πρώιμο στάδιο και θα κάνει δυνατή την διεπιστημονική ανταλλαγή. Αυτό θα συνεχιστεί με την νομική αξιολόγηση των πιλοτικών εφαρμογών. Με αυτόν τον τρόπο διασφαλίζεται η νομική συμμόρφωση με τις οδηγίες για την προστασία των δεδομένων.

5 Ηλεκτρονικές ταυτότητες

5.1 Οι νόμοι της ταυτότητας

Το θέμα των ηλεκτρονικών ταυτοτήτων είναι αντικείμενο γενικότερης συζήτησης. Σε αυτό το κεφάλαιο θα παρουσιάσουμε τους νόμους ταυτότητας του Cameron, θα γνωρίσουμε την ιταλική και την γερμανική ηλεκτρονική ταυτότητα και θα περιγράψουμε 4 πιθανά σενάρια που για να υλοποιηθούν απαιτείται η ανάπτυξη κατάλληλων υπηρεσιών ψηφιακών ταυτοτήτων σε συνδυασμό με πλήρη αξιοποίηση των δυνατοτήτων που προσφέρει το «νέφος».

Μια έννοια που σχετίζεται άμεσα με τη ιδιωτικότητα είναι εκείνη της ταυτότητας. Αλλά τι ονομάζουμε ταυτότητα στον ψηφιακό κόσμο; Σύμφωνα με το Fidis [21] η *ταυτότητα* (identity) είναι μια δομή που αντιμετωπίζεται σαν ένα σύνολο χαρακτηριστικών που χαρακτηρίζουν ένα άτομο σ' ένα συγκεκριμένο πλαίσιο. Ενώ η *ταυτοποίηση* (identification) θεωρείται ένα σύνολο διαδικασιών που σχετίζονται με την αποκάλυψη πληροφοριών για ένα άτομο αλλά και χρήση αυτών των πληροφοριών. Κάθε χώρα έχει υιοθετήσει έναν τρόπο ώστε να καταγράφει και να διαχωρίζει μοναδικά κάθε πολίτη (π.χ. με τις παραδοσιακές ταυτότητες) Στην πραγματικότητα όμως ένα άτομο έχει πολλές διαφορετικές ταυτότητες (π.χ. ως πολίτης, ως εργαζόμενος, ως καταναλωτής, ως πελάτης, ως ασθενής, κλπ.).

Στον κόσμο του Διαδικτύου πολύ συχνά φυσικά ή εικονικά πρόσωπα ζητούν πρόσβαση σε δεδομένα ή υπηρεσίες. Οι πάροχοι υπηρεσιών πρέπει να πιστοποιήσουν την αυθεντικότητά τους σε κάποιον πελάτη. Για να γίνει αυτό τα εμπλεκόμενα μέρη συχνά χρειάζεται να αποδείξουν συγκεκριμένους ισχυρισμούς για τους ίδιους ώστε να πείσουν το άλλο μέρος (πάροχος δεδομένων ή υπηρεσιών, εργαζόμενος, πελάτης) να τους εμπιστευτεί αρκετά ώστε να επιτρέψει να πραγματοποιηθεί η συναλλαγή, ανταλλαγή πληροφοριών ή επικοινωνία. Τέτοιοι ισχυρισμοί μπορεί να περιλαμβάνουν για παράδειγμα: όνομα, ημερομηνία γέννησης, ηλικία, αριθμό πιστωτικής κάρτας, βιομετρικά στοιχεία.

Σύμφωνα με την Wikipedia η ηλεκτρονική ταυτότητα είναι ένα επίσημο «έγγραφο» που εκδίδεται από την κυβέρνηση μιας χώρας για online και offline ταυτοποίηση.

[21] http://www.fidis.net/

Εκτός από την online ταυτοποίηση, πολλές ηλεκτρονικές ταυτότητες δίνουν την δυνατότητα στους χρήστες να υπογράφουν ηλεκτρονικά έγγραφα χρησιμοποιώντας ψηφιακές υπογραφές. Η ηλεκτρονική ταυτότητα έχει την μορφή μιας κοινής τραπεζικής κάρτας, με τυπωμένα πάνω της κάποια στοιχεία του κατόχου (όπως ονοματεπώνυμο και φωτογραφία) και ενσωματωμένο μικροτσίπ.

Ο Kim Cameron το 2005 παρουσίασε τους νόμους της ταυτότητας [33]. Σαφώς οι ισχυρισμοί που παρέχονται για μια συγκεκριμένη συναλλαγή εξαρτώνται από την συναλλαγή, τα εμπλεκόμενα μέρη και το πλαίσιο μέσα στο οποίο πραγματοποιείται η συναλλαγή. Η *ανωνυμία* (anonymity) αναφέρεται στην απουσία ταυτοποίησης πληροφοριών που σχετίζονται μ' ένα φυσικό πρόσωπο. Σε τέτοιες περιπτώσεις δεν παρέχονται ισχυρισμοί που επιτρέπουν την ταυτοποίηση, παρόλο που μπορεί να είναι απαραίτητοι άλλοι ισχυρισμοί. Στην *ψευδωνυμία* (pseudonymity) παρέχονται συγκεκριμένοι ισχυρισμοί (για παράδειγμα, ένας αριθμός ή ένα login name και ένας κωδικός πρόσβασης), αλλά δεν μπορούν να συνδυαστούν μεταξύ τους ώστε να γίνει άμεσα ταυτοποίηση. Παρόλα αυτά το φυσικό πρόσωπο μπορεί να ταυτοποιηθεί εάν κριθεί απαραίτητο.

1. **Έλεγχος χρήστη και συγκατάθεση**: Τα συστήματα ταυτοποίησης πρέπει να αποκαλύπτουν πληροφορίες που ταυτοποιούν έναν χρήστη μόνο με την συγκατάθεσή του.
2. **Ελάχιστη αποκάλυψη για μια περιορισμένη χρήση**: Η λύση που αποκαλύπτει το ελάχιστο ποσό πληροφορίας για την ταυτοποίηση κάποιου ατόμου και περιορίζει με τον καλύτερο τρόπο την χρήση της είναι η πιο μόνιμη μακροπρόθεσμη λύση.
3. **Αιτιολογούμενα μέρη**: Τα ψηφιακά συστήματα ταυτότητας πρέπει να είναι σχεδιασμένα έτσι ώστε οι πληροφορίες ταυτοποίησης που αποκαλύπτονται να περιορίζονται στα μέρη που έχουν μια αναγκαία και αιτιολογημένη θέση σε μια δεδομένη σχέση που απαιτεί ταυτοποίηση. Το σύστημα ταυτοτήτων πρέπει να ενημερώνει τον χρήστη για το μέρος ή τα μέρη με τα οποία αλληλεπιδρά όταν ανταλλάσσει πληροφορίες. Η απαίτηση για αιτιολόγηση ισχύει τόσο για το μέρος που αποκαλύπτει κάποια πληροφορία όσο και για το μέρος που εξαρτάται από αυτήν.
4. **Κατευθυνόμενη ταυτότητα**: Ένα ενιαίο σύστημα ταυτοτήτων πρέπει να υποστηρίζει "πολλαπλών κατευθύνσεων" αναγνωριστικά για χρήση από

δημόσιες οντότητες και "μίας κατεύθυνσης" αναγνωριστικά για χρήση από ιδιωτικές οντότητες.

5. **Πλουραλισμός των διαχειριστών και των τεχνολογιών**: Ένα ενιαίο σύστημα ταυτοτήτων πρέπει να διοχετεύσει και να επιτρέψει την διαλειτουργικότητα των διάφορων τεχνολογιών ταυτότητας που ανήκουν σε διαφορετικούς παρόχους ταυτοτήτων.
6. **Ανθρώπινη ολοκλήρωση:** Το ενιαίο μετασύστημα ταυτοτήτων πρέπει να ορίσει τον ανθρώπινο χρήστη ως ένα στοιχείο του κατανεμημένου συστήματος, το οποίο ολοκληρώνεται μέσα από μη διφορούμενους μηχανισμούς επικοινωνίας ανθρώπου-μηχανής, που προσφέρουν προστασία από επιθέσεις ταυτότητας.
7. **Συνέπεια σε διαφορετικές χρήσεις:** Το ενοποιημένο μετασύστημα ταυτοτήτων πρέπει να εξασφαλίσει στους χρήστες του μια απλή συνεπής εμπειρία, ενώ θα επιτρέπει των διαχωρισμό των περιβαλλόντων μέσω πολλαπλών διαχειριστών και τεχνολογιών.

Εικόνα 5. Οι Νόμοι της Ταυτότητας

5.2 Η ιταλική ηλεκτρονική ταυτότητα

Η Carta d'Identità Elettronica[22] (στην Ιταλία χρησιμοποιείται το ακρωνύμιο CIE), αποτελεί ένα προσωπικό «έγγραφο» ταυτοποίησης που αντικαθιστά το έντυπο δελτίο ταυτότητας. Οι πρώτες ιταλικές ηλεκτρονικές ταυτότητες εκδόθηκαν το 2001. Από 1η Ιανουαρίου 2006 η ιταλική κυβέρνηση επέβαλλε την αντικατάσταση των συμβατικών ταυτοτήτων με ηλεκτρονικές.

Η ιταλική ηλεκτρονική ταυτότητα προορίζεται για online και offline ταυτοποίηση. Ως εκ τούτου, εκτός από τις τυπωμένες πληροφορίες, αποθηκεύονται σ' ένα μικροτσίπ δεδομένα που χρησιμοποιούνται για ταυτοποίηση του κατόχου της ηλεκτρονικής ταυτότητας. Συγκεκριμένα, το μικροτσίπ περιέχει ένα ψηφιακό πιστοποιητικό για online αυθεντικοποίηση και (προαιρετικά) ένα πιστοποιητικό για ψηφιακές υπογραφές. Η ιταλική ηλεκτρονική ταυτότητα έχει σχεδιαστεί αποκλειστικά για να

[22]Περισσότερα στην διεύθυνση www.halnet.it/cie/

προσφέρει πρόσβαση σε υπηρεσίες ηλεκτρονικής διακυβέρνησης, και θα αποτελέσει το πρότυπο για πρόσβαση σε online υπηρεσίες που προσφέρονται στους Ιταλούς πολίτες από δημόσιες αρχές. Η ιταλική ηλεκτρονική ταυτότητα περιέχει τα παρακάτω πεδία:

1. Δήμος έκδοσης
2. Επώνυμο
3. Όνομα
4. Τόπος γέννησης
5. Ημερομηνία γέννησης
6. Φύλο
7. Αριθμός πιστοποιητικού γεννήσεως
8. Ύψος
9. Δήμος κατοικίας
10. Διεύθυνση
11. Ημερομηνία έκδοσης
12. Ημερομηνία λήξης
13. Ιθαγένεια
14. Αριθμός φορολογικού μητρώου
15. Υπογραφή

Η κάρτα περιέχει επίσης:

- Το λογότυπο της Ιταλικής Δημοκρατίας
- Έναν μοναδικό αριθμό ταυτοποίησης της κάρτας
- Φωτογραφία του κατόχου της κάρτας
- Ολόγραμμα ασφάλειας
- Ταινία laser

Το μικροτσίπ περιέχει όλες τις πληροφορίες που είναι τυπωμένες πάνω στην κάρτα, την ψηφιακή εκδοχή της φωτογραφίας του κατόχου της κάρτας και τα ψηφιακά πιστοποιητικά που εκδίδονται από την Αρχή Πιστοποίησης του ιταλικού Υπουργείου Εσωτερικών. Στο τσιπ περιέχονται προαιρετικά δαχτυλικά αποτυπώματα και η υποδομή που απαιτείται για τις ψηφιακές υπογραφές. Η ιταλική ηλεκτρονική ταυτότητα είναι περισσότερο μια ψηφιοποίηση της συμβατικής ταυτότητας, ενώ

αναμένεται να αποτελέσει το πρότυπο για την επικείμενη ελληνική ηλεκτρονική ταυτότητα.

Εικόνα 6. Η ιταλική ηλεκτρονική ταυτότητα

5.3 Η γερμανική ηλεκτρονική ταυτότητα

Από το 2010 η γερμανική ταυτότητα είναι ηλεκτρονική[23]. Η ηλεκτρονική ταυτότητα (στα γερμανικά Personalausweis) εκδίδεται στους Γερμανούς πολίτες από τα τοπικά εξουσιοδοτημένα γραφεία. Είναι υποχρεωτικό όλοι οι Γερμανοί πολίτες που είναι 16 ετών και άνω να διαθέτουν ταυτότητα ή διαβατήριο αλλά όχι απαραίτητα να τα έχουν πάντα μαζί τους. Η γερμανική ταυτότητα έχει ισχύ 10 χρόνια. Σε αντίθεση με άλλες χώρες δεν υπάρχει κεντρική βάση δεδομένων που να περιέχει όλους τους κατόχους ηλεκτρονικών ταυτοτήτων. Το ονοματεπώνυμο, η ημερομηνία γέννησης και η διεύθυνση του κατόχου της ταυτότητας αποθηκεύονται μόνο στο τοπικό γραφείο, ενώ η φωτογραφία, τα δαχτυλικά αποτυπώματα, η υπογραφή και πληροφορίες για το χρώμα των ματιών και το ύψος καταστρέφονται αμέσως μετά την δημιουργία της ηλεκτρονικής ταυτότητας.

Οι σημερινές ηλεκτρονικές ταυτότητες τύπου 1 διατίθενται από τον Νοέμβριο του 2010. Περιέχουν ένα τσιπ RFID (Radio-frequency identification)[24] παρόμοιο με αυτό που υπάρχει στα βιομετρικά διαβατήρια. Το τσιπ περιέχει τις πληροφορίες που αναγράφονται στην ταυτότητα (όπως όνομα ή ημερομηνία γέννησης), την

[23] Περισσότερα στην διεύθυνση www.personalausweisportal.de/DE/Home/home_node.html
[24] Είναι μια τεχνολογία που χρησιμοποιεί την επικοινωνία μέσω ραδιοκυμάτων για την ανταλλαγή δεδομένων ανάμεσα σ' έναν αναγνώστη και μια ετικέτα που έχει προσαρτηθεί σ' ένα αντικείμενο με σκοπό τον εντοπισμό και την αναγνώριση του αντικειμένου.

φωτογραφία του κατόχου (που σε αντίθεση με άλλες ηλεκτρονικές ταυτότητες πρέπει να είναι βιομετρική), και επιπλέον αν ο χρήστης επιθυμεί, τα δαχτυλικά του/της αποτυπώματα. Το μπροστινό τμήμα της ταυτότητας περιέχει τις παρακάτω πληροφορίες:

1. Φωτογραφία (βιομετρική) του κατόχου της ταυτότητας
2. Αριθμός της ταυτότητας
3. Κωδικός πρόσβασης για το RFID τσιπ
4. Επίθετο
5. Όνομα
6. Ημερομηνία γέννησης
7. Εθνικότητα
8. Τόπος γέννησης
9. Ημερομηνία λήξης
10. Υπογραφή του κατόχου

Ενώ στο πίσω μέρος αναγράφονται:

1. Χρώμα ματιών
2. Ύψος
3. Ημερομηνία έκδοσης
4. Εκδούσα αρχή
5. Διεύθυνση κατοικίας
6. Θρησκευτικό όνομα ή ψευδώνυμο (εάν ο χρήστης έχει)
7. Ζώνη αναγνωρίσιμη από μηχάνημα (machine-readable zone), δηλαδή περιοχή που αναγράφει κωδικοποιημένες πληροφορίες οι οποίες μπορούν να αναγνωσθούν μόνο με οπτική ανάγνωση χαρακτήρων (OCR)

Η νέα ηλεκτρονική ταυτότητα χρησιμοποιεί υδατογραφήματα (guillochés), μικροεκτύπωση[25], βαφές φθορισμού[26], πολύχρωμες ίνες φθορισμού, και άλλα χαρακτηριστικά συμπεριλαμβανομένων έγχρωμα φθορίζων υδατογραφήματα, μελάνι που αλλάζει χρώμα ανάλογα από ποια γωνία κοιτά κανείς την ταυτότητα,

[25] Περιλαμβάνει την χρήση εξαιρετικά μικρού μεγέθους κειμένου, και χρησιμοποιείται συχνά σε επιταγές. Το κείμενο είναι τόσο μικρό ώστε να μην διακρίνεται με γυμνό μάτι.
[26] Βαφές φθορισμού είναι βαφές που φθορίζουν κάτω από υπεριώδες φως ή ασυνήθιστο φωτισμό. Εμφανίζονται ως λέξεις, μοτίβα ή εικόνες και μπορεί να είναι ορατά ή όχι σε κανονικό φωτισμό. Το χαρακτηριστικό αυτό συχνά ενσωματώνεται σε χαρτονομίσματα

προσωποποιημένο (δηλαδή το όνομα του κατόχου και ο αριθμός της κάρτας είναι τυπωμένα πάνω σε αυτό) νήμα ασφάλειας (security thread)[27].

Μπορεί να χρησιμοποιηθεί για online αυθεντικοποίηση (π.χ. για να εξακριβωθεί αν ένας χρήστης είναι 18 ετών ή για εφαρμογές ηλεκτρονικής διακυβέρνησης). Για να χρησιμοποιήσει την online αυθεντικοποίηση ο κάτοχος της ταυτότητας, χρειάζεται ένα εξαψήφιο αριθμό PIN. Εάν ο χρήστης πληκτρολογήσει λάθος PIN, πρέπει στην συνέχεια να πληκτρολογήσει τον εξαψήφιο κωδικό πρόσβασης που αναγράφεται πάνω στη ταυτότητα ώστε να αποδείξει πως είναι πράγματι ο κάτοχός της. Εάν εισαχθεί 3 φορές λάθος ο αριθμός PIN, τότε απαιτείται ο αριθμός PUK. Οι πληροφορίες στο τσιπ προστατεύονται από Βασικό Έλεγχο Πρόσβασης (Basic Access Control)[28] και Εκτεταμένο Έλεγχο Πρόσβασης (Extended Access Control)[29]. Στο τσιπ μπορεί επίσης να αποθηκευτεί ψηφιακή υπογραφή που παρέχεται από κάποια ιδιωτική εταιρεία. Σύμφωνα με την γερμανική κυβέρνηση η νέα ταυτότητα επιτρέπει στις γερμανικές αρχές να εντοπίζουν ανθρώπους με ακρίβεια και ταχύτητα. Τέτοιες αρχές είναι η αστυνομία, τελωνειακές και φορολογικές αρχές και αρχές έκδοσης διαβατηρίων.

Εικόνα 7. Η γερμανική ηλεκτρονική ταυτότητα

[27] Ένα νήμα ασφάλειας είναι ένα χαρακτηριστικό πολλών χαρτονομισμάτων για προστασία από την παραχάραξη, και αποτελείται από μια λεπτή ταινία που βρίσκεται μέσα στο χαρτί του χαρτονομίσματος

[28] Βασικός Έλεγχος Πρόσβασης είναι ένας μηχανισμός που χρησιμοποιείται για να εξασφαλίσει πως μόνο εξουσιοδοτημένα μέρη μπορούν να διαβάσουν ασύρματα προσωπικές πληροφορίες από διαβατήρια χρησιμοποιώντας ένα RFID τσιπ.

[29] Εκτεταμένος Έλεγχος Πρόσβασης είναι ένας μηχανισμός που επιτρέπει μόνο σε ένα εξουσιοδοτημένο σύστημα που χρησιμοποιείται για την ανάγνωση των ηλεκτρονικών διαβατηρίων, να διαβάσει βιομετρικά δεδομένα όπως δαχτυλικά αποτυπώματα.

Διαφαίνεται πως στο μέλλον στις περισσότερες ευρωπαϊκές χώρες οι συμβατικές ταυτότητες θα αντικατασταθούν με τις ηλεκτρονικές ταυτότητες. Εκτός από την Ιταλία και την Γερμανία άλλες χώρες που έχουν εκδώσει ή πρόκειται να εκδώσουν στο άμεσο μέλλον ηλεκτρονικές ταυτότητες είναι το Βέλγιο, η Ρουμανία, η Ολλανδία, η Φιλανδία, η Εσθονία, η Αυστρία, η Πορτογαλία και η Ισπανία. Κάνοντας μια γρήγορη επισκόπηση (δομή, περιεχόμενες πληροφορίες, δυνατότητες και λειτουργίες) της ιταλικής και της γερμανικής ηλεκτρονικής ταυτότητας αλλά και των υπόλοιπων, διαπιστώνει κανείς διαφοροποιήσεις από χώρα σε χώρα. Αυτό δεν έχει να κάνει μόνο με τις κυβερνητικές αποφάσεις που αφορούν την μορφή της ηλεκτρονικής ταυτότητας αλλά και με την άρνηση των πολιτών ορισμένων χωρών, όπως του Ηνωμένου Βασιλείου, για καταγραφή δεδομένων προσωπικού χαρακτήρα, ενώ άλλες χώρες, όπως η Ιταλία, θα τις χαρακτηρίζαμε περισσότερο διαλλακτικές.

5.4 «Νέφος» και ψηφιακή ταυτότητα

Το Διαδίκτυο έχει περάσει σε μια νέα εποχή. Ορόσημο σε αυτή την νέα εποχή αποτελεί το «νέφος». Σε προηγούμενο κεφάλαιο αναφέραμε κάποια από τα πιθανά οφέλη του σε επιχειρήσεις και μεμονωμένους χρήστες. Όμως για να μπορούμε να απολαμβάνουμε πλήρως αυτά τα οφέλη πρέπει πρώτα να αντιμετωπιστούν τα ζητήματα ασφάλειας και ιδιωτικότητας τα οποία προκύπτουν από την αποθήκευση ευαίσθητων προσωπικών δεδομένων σε βάσεις δεδομένων και λογισμικά που βρίσκονται διάσπαρτα στο Διαδίκτυο.

Η ψηφιακή ταυτότητα αποτελεί βασική πρόκληση στο «νέφος». Στην πρώτη φάση της εμπορικής χρήσης των υπολογιστών το λειτουργικό σύστημα, τα δεδομένα και τα λογισμικά που ο χρήστης χρησιμοποιούσε αποθηκεύονταν σ’ ένα μόνο μηχάνημα. Η ιδιωτικότητα και η ασφάλεια του χρήστη ήταν σε μεγάλο βαθμό εξασφαλισμένη, περιορίζοντας την φυσική πρόσβαση σε μεμονωμένες (stand-alone) υπολογιστικές συσκευές και μέσα αποθήκευσης. Οι ανάγκες για ταυτοποίηση ήταν λιγοστές, και αφορούσαν κυρίως την χρήση usernames και passwords για πρόσβαση σε τοπικά συστήματα και αρχεία. Στην συνέχεια με την εμφάνιση του Web, τα περισσότερα λογισμικά που ένας χρήστης χρειάζεται, συνεχίζουν να υπάρχουν στον δικό του

υπολογιστή, αλλά τα περισσότερα δεδομένα βρίσκονται πλέον στο Διαδίκτυο (π.χ. η χρήση ενός Web browser για να διαβαστεί μια ιστοσελίδα).

Με τον ερχομό του «νέφους» προέκυψαν ακόμα περισσότερες αλλαγές. Σήμερα, σχεδόν όλες οι online δραστηριότητες που πραγματοποιούμε καθημερινά, όπως αποστολή email, κατάθεση φορολογικών δηλώσεων, διαχείριση τραπεζικών λογαριασμών, αγορά προϊόντων, παιχνίδια, σύνδεση στο Intranet μιας εταιρείας και εικονικοί κόσμοι, απαιτούν να δώσουμε πληροφορίες που αφορούν την ταυτότητά μας. Ο χρήστης λοιπόν, πρέπει να δημιουργεί την ταυτότητά του κάθε φορά που χρησιμοποιεί μια web based εφαρμογή, συμπληρώνοντας συνήθως μια online φόρμα με ευαίσθητα προσωπικά δεδομένα (π.χ. όνομα, διεύθυνση κατοικίας, αριθμός πιστωτικής κάρτας, αριθμός τηλεφώνου κλπ.). Μ’ αυτόν τον τρόπο αφήνει στον ψηφιακό κόσμο ίχνη από τις προσωπικές πληροφορίες που αποκαλύπτει, οι οποίες μπορούν στην συνέχεια, εάν δεν προστατεύονται πλήρως, να χρησιμοποιηθούν για κακόβουλες και παράνομες δραστηριότητες. Εάν στα προσωπικά δεδομένα συμπεριλάβουμε τα cookies και τις διευθύνσεις IP τότε τα πράγματα δυσχεραίνουν ακόμα περισσότερο.

Θα λέγαμε λοιπόν πως το «νέφος» χρειάζεται υπηρεσίες ταυτότητας που:

- Να είναι ανεξάρτητες από τις συσκευές
- Να επιτρέπουν στον χρήστη να δημιουργεί έναν μόνο λογαριασμό (sign-on) και να τον χρησιμοποιεί στις χιλιάδες διαφορετικές online υπηρεσίες
- Να επιτρέπουν σε ψευδώνυμα και πολλαπλές διακριτές (αλλά έγκυρες) ταυτότητες να προστατεύουν την ιδιωτικότητα του χρήστη
- Να είναι διαλειτουργικές, να βασίζονται σε ανοιχτά πρότυπα και να είναι διαθέσιμα σε open source λογισμικό
- Να επιτρέπουν μια ενοποιημένη διαχείριση ταυτοτήτων
- Να είναι διαφανείς και ελέγξιμες.

Στην συνέχεια περιγράφονται 4 πιθανά σενάρια, που για να υλοποιηθούν απαιτείται η ανάπτυξη κατάλληλων υπηρεσιών ψηφιακών ταυτοτήτων σε συνδυασμό με πλήρη αξιοποίηση των δυνατοτήτων που προσφέρει το «νέφος».[34]

5.4.1 “Live Web”

Στις μέρες μας το Web είναι περισσότερο αλληλεπιδραστικό από ποτέ. Αυτό προκύπτει άλλωστε και από τον μεγάλο αριθμό αναρτήσεων σε blogs, το πλήθος των συνεργατικών wikis και του συνεχώς αυξανόμενου αριθμού των χρηστών σελίδων κοινωνικής δικτύωσης. Το φαινόμενο του «συμμετοχικού Web» έχει αλλάξει τις ζωές μας, προσφέροντάς μας σχεδόν απεριόριστες δυνατότητες. Απαιτείται όμως προσεχτική διαχείριση της ταυτότητας των χρηστών. Οι χρήστες πρέπει να μπορούν να διαχειρίζονται με ασφάλεια τους πολλούς λογαριασμούς και κωδικούς που πιθανώς να διαθέτουν σε διαφορετικούς τομείς, χωρίς τον κίνδυνο να μπορεί κάποιος να σκιαγραφήσει το προφίλ τους ή να παρακολουθεί τις online δραστηριότητές τους.

Για να γίνει πιο εύκολα αυτό, το OpenID, είναι μια τεχνολογία ψηφιακής ταυτότητας που έχει ως επίκεντρό της τον χρήστη, και που απλοποιεί την online εμπειρία του χρήστη μειώνοντας την πολυπλοκότητα του να διαχειρίζεται δεκάδες, ή ακόμα και εκατοντάδες user names και passwords, προσφέροντας έτσι μεγαλύτερο έλεγχο στις προσωπικές πληροφορίες που χρειάζεται οι χρήστες να μοιραστούν όταν συνδέονται σε κάποια υπηρεσία ή εφαρμογή.

Το OpenID επιτρέπει στους χρήστες να μετατρέψουν ένα από τα ήδη υπάρχοντα αναγνωριστικά τους - όπως το URL του προσωπικού τους blog - σ’ έναν λογαριασμό OpenID, που μπορεί στην συνέχεια να χρησιμοποιηθεί ως log-in σε οποιοδήποτε άλλο δικτυακό τόπο που υποστηρίζει την τεχνολογία OpenID. Όσο αφορά τις online επιχειρήσεις, τέτοιες προσπάθειες μπορούν να μειώσουν το κόστος διαχείρισης λογαριασμών και κωδικών πρόσβασης. Επίσης συμβάλλουν στην μείωση των κινδύνων από παραβιάσεις ασφάλειας με την μείωση του ποσού των προσωπικών πληροφοριών των χρηστών που πρέπει να αποθηκεύονται και να προστατεύονται.

5.4.2 Online Dating

Μια online υπηρεσία ραντεβού ‘‘ταιριάζει’’ ανθρώπους με βάση τα ενδιαφέροντά και τις προτιμήσεις τους, χρησιμοποιώντας πολύπλοκους αλγόριθμους. Ο αλγόριθμος απαιτεί καλό χειρισμό των δεδομένων ώστε να είναι αποτελεσματικός, έτσι οι

χρήστες τέτοιων υπηρεσιών χρειάζονται εγγυήσεις πως τα προσωπικά τους δεδομένα θα χρησιμοποιηθούν μόνο για τον συγκεκριμένο σκοπό.

Μπορεί κάποιος χρήστης να συμφωνεί για παράδειγμα στο να λαμβάνει διαφημιστικά mail από τρίτους, θέλει όμως να είναι σίγουρος πως οι προσωπικές του πληροφορίες δεν θα αποκαλύπτονται σε αυτούς. Για παράδειγμα, κάποιος που είναι υπέρβαρος μπορεί να μην επιθυμεί να λαμβάνει διαφημιστικά mail από εταιρείες που κατασκευάζουν ρούχα σε μεγάλα μεγέθη.

Για να προστατευθεί η ιδιωτικότητα, οι υπηρεσίες ραντεβού θα μπορούσαν να επιτρέπουν στους πελάτες τους να χρησιμοποιούν ψευδώνυμα αντί για τα πραγματικά τους ονόματα. Τέτοιες υπηρεσίες δεν είναι απαραίτητο να γνωρίζουν την πραγματική ταυτότητα των πελατών τους, μόνο το ότι τελικά θα πληρωθούν, κάτι το οποίο μπορεί να γίνει προπληρώνοντας ο πελάτης για τις υπηρεσίες που θα λάβει.

Σήμερα οι πελάτες τέτοιων υπηρεσιών μπορούν να ισχυριστούν πως διαθέτουν οποιοδήποτε χαρακτηριστικό, και ως εκ τούτου ένας "διάβολος" μπορεί να παρουσιαστεί ως "άγγελος". Με καλύτερη διαχείριση της ψηφιακής ταυτότητας των χρηστών, η υπηρεσία ραντεβού θα μπορεί να αποδεχθεί χαρακτηριστικά που πιστοποιούνται από τρίτους. Αυτό θα γινόταν χωρίς οι πελάτες τους να διατρέχουν τον κίνδυνο να αποκαλύψει το πιστοποιητικό στην υπηρεσία ραντεβού τα πραγματικά τους ονόματα. Μια τέτοια προσέγγιση θα μείωνε τον κίνδυνο του να παρουσιαστεί κάποιος διαφορετικός απ' ότι είναι. Θα αυξανόταν έτσι το επίπεδο της εμπιστοσύνης ανάμεσα στους πελάτες και την υπηρεσία χωρίς να υπάρχουν επιπτώσεις για την ιδιωτικότητα.

5.4.3 Ηλεκτρονικά ιατρικά μητρώα

Μερικές από τις πιο ευαίσθητες προσωπικές πληροφορίες που αφορούν καθέναν από εμάς σχετίζεται με τις ιατρικές υπηρεσίες που χρησιμοποιούμε και τα φάρμακα που λαμβάνουμε. Σήμερα διάφορες προσωπικές μας πληροφορίες είναι διασκορπισμένες σε διαφορετικές θέσεις όπως ιατρεία, φαρμακεία και ασφαλιστικές εταιρείες. Ένα από τα μεγαλύτερα εμπόδια για την ευρεία υιοθέτηση των ηλεκτρονικών μητρώων υγείας είναι η ανησυχία των ασθενών πως τα δεδομένα τους σε τέτοια αρχεία θα

κλαπούν ή θα χρησιμοποιηθούν με λανθασμένο τρόπο. Ήδη υπάρχουν παραδείγματα ευαίσθητων ιατρικών δεδομένων που έχουν χρησιμοποιηθεί για παράνομους σκοπούς. Μια διαχείριση ταυτότητας που θα έχει στο επίκεντρό της τον χρήστη (χρηστοκεντρική δηλαδή) θα μπορούσε να εξασφαλίσει πως το πραγματικό όνομα κάποιου (και τα προσωπικά δεδομένα που θα μπορούσαν να χρησιμοποιηθούν για να συμπεράνουμε ποιος είναι), θα προστατευόταν και θα διατηρούνταν ξεχωριστά από τα στοιχεία του ηλεκτρονικού ιατρικού του φακέλου. Θα επέτρεπε σ' έναν ασθενή να χρησιμοποιήσει μια online πύλη μ' ένα ενοποιημένο σύστημα ταυτότητας για να μπορεί να έχει γρήγορη και ασφαλή πρόσβαση σε όλες τις ιατρικές του πληροφορίες, είτε είναι αποθηκευμένες στο γραφείο του γιατρού του, είτε στο φαρμακείο που είναι πελάτης, είτε στα γραφεία της ασφαλιστικής του εταιρείας. Ίσως το πιο σημαντικό είναι πως θα μπορούσε να ελέγχει αυτά τα αρχεία, και να καθορίσει που θα αποθηκευτούν τα προσωπικά του δεδομένα, πως θα προστατεύονται, και ποιος θα έχει πρόσβαση σε αυτά.

5.4.4 Ταυτότητα και αξιοπιστία στους εικονικούς κόσμους

Εκατομμύρια άνθρωποι ξοδεύουν πολλές ώρες την εβδομάδα σε εικονικά τρισδιάστατα περιβάλλοντα, ανακαλύπτοντας νέους τρόπους να συνεργάζονται, να παίζουν παιχνίδια και να μοιράζονται πληροφορίες. Μέσα σε εικονικούς κόσμους (Virtual Worlds) αναπτύσσονται εικονικές οικονομίες ως μέρος του παιχνιδιού, αγοράζοντας και πουλώντας εικονικά προϊόντα και υπηρεσίες, ενώ ανταλλάσσονται εκατομμύρια πραγματικών δολαρίων κάθε χρόνο.

Δυστυχώς δεν υπάρχουν ακόμα αποτελεσματικά μέσα για την διαχείριση της ταυτότητας και της ασφάλειας στους περισσότερους εικονικούς κόσμους. Ως εκ τούτου, είναι δύσκολο να αποφευχθεί η ανάρμοστη συμπεριφορά ή ακατάλληλες δημοσιεύσεις (postings) από ανώνυμους χρήστες που μπορεί να εμφανιστούν και να εξαφανιστούν αμέσως. Αυτή η έλλειψη ασφάλειας και εμπιστοσύνης επιβραδύνει την ανάπτυξη σοβαρών επιχειρηματικών εφαρμογών σε εικονικούς κόσμους.

Η χρηστοκεντρική διαχείριση ταυτότητας θα μπορούσε να προσφέρει έναν αποτελεσματικό τρόπο για την δημιουργία έμπιστων κοινοτήτων σε εικονικούς κόσμους. Για παράδειγμα, οι γονείς θα μπορούσαν να είναι ήσυχοι πως όταν τα

παιδιά τους είναι online για να παίξουν σ' ένα εικονικό κόσμο για παιδιά, έχει γίνει έλεγχος της ταυτότητας όλων των άλλων παιχτών και είναι πράγματι παιδιά.

Ένας από τους πιο συναρπαστικούς λόγους για την εντυπωσιακή αύξηση των εικονικών κόσμων, όπως το Second Life, είναι ότι επιτρέπουν στους χρήστες να δημιουργούν νέες υπηρεσίες και να "ενσωματώνουν" εφαρμογές από οπουδήποτε αλλού στο Web. Με την χρηστοκεντρική διαχείριση ταυτότητας, θα μπορούσαν οι χρήστες να δημιουργήσουν την ταυτότητά τους μία φορά και μετά να μπορούν να χρησιμοποιήσουν μια πληθώρα υπηρεσιών σ' ένα εικονικό κόσμο. Επίσης μια ταυτότητα που θα δημιούργησε κάποιος χρήστης στο Second Life θα μπορούσε να μεταφερθεί και σ' έναν άλλον εικονικό κόσμο. Αλλά δεν θα χρειαζόταν να μοιραστεί τις προσωπικές του πληροφορίες σε οποιονδήποτε άλλο "κόσμο", εκτός και αν το επιλέξει.

6 Συμπεράσματα – Προοπτικές

Το «νέφος» είναι πλέον πραγματικότητα και το Cromebook είμαι μια ζωντανή απόδειξη. Τα Chromebooks θα είναι διαθέσιμα για αγορά ή ενοικίαση από τις 15 Ιουνίου 2011 στο Amazon και το Best Buy στην Αμερική. Στην Ευρώπη το Chromebook θα κυκλοφορήσει την ίδια ημερομηνία σε Αγγλία, Γαλλία, Γερμανία, Ολλανδία, Ιταλία και Ισπανία ενώ οι υπόλοιπες χώρες θα ακολουθήσουν αργότερα.

Με πολύ γρήγορο ρυθμό οι υπηρεσίες του «νέφους» διευρύνονται και βρίσκουν όλο και περισσότερες εφαρμογές στην καθημερινότητά μας. Όμως τα ζητήματα ιδιωτικότητας που προκύπτουν αποτελούν μεγάλο αγκάθι σε αυτή την εξάπλωση. Μόνο όταν οι χρήστες νοιώσουν πως τα δεδομένα τους είναι ασφαλή και προστατεύεται επαρκώς η ιδιωτικότητα τους θα αξιοποιήσουν πλήρως τις δυνατότητες που το «νέφος» έχει να προσφέρει.

Μια πιθανή λύση είναι οι νέας μορφής ηλεκτρονικές ταυτότητες, οι οποίες δίνουν την δυνατότητα στους χρήστες να αποκαλύπτουν μόνο τα δεδομένα που είναι απαραίτητα, να πραγματοποιείται δηλαδή αυτό που ονομάζουμε *ελάχιστη αποκάλυψη*. Για παράδειγμα, όταν κάποιος χρήστης επιθυμεί να ενοικιάσει ένα αυτοκίνητο, η εταιρεία ενοικίασης αρκεί να επικυρώσει το γεγονός πως ο χρήστης είναι ενήλικος και έχει δίπλωμα οδήγησης. Επιπλέον πληροφορίες όπως η ημερομηνία γέννησης του χρήστη ή ο αριθμός διπλώματος οδήγησης, δεν είναι απαραίτητο να αποκαλυφθούν. Σαφώς, σε περίπτωση που αυτό κριθεί σκόπιμο π.χ. σε περίπτωση ατυχήματος, η αποκάλυψη περισσότερων δεδομένων του χρήστη είναι αναπόφευκτη.

Ήδη υπάρχουν χώρες που έχουν προχωρήσει ένα βήμα παραπάνω και οι ηλεκτρονικές ταυτότητες που έχουν υιοθετήσει δεν είναι απλά προϊόν ψηφιοποίησης των συμβατικών ταυτοτήτων. Καθώς αυτή η προσπάθεια θα συνεχίζεται, όλο και περισσότερα ερευνητικά προγράμματα, όπως το ABC4Trust, θα προσπαθούν να καθορίσουν κοινά πρότυπα, όπως ένα πλαίσιο για την ενοποίηση και εναλλαξιμότητα διαφόρων υπαρχόντων και νέων τεχνολογιών αλλά και τον καθορισμό ακριβών και πλήρων μετρικών για την σύγκριση συστημάτων που ήδη υπάρχουν και που σίγουρα θα προκύψουν στο μέλλον.

Η ιδιωτικότητα των δεδομένων τέμνει επίσης την ανάπτυξη του σημασιολογικού ιστού και των συνδεδεμένων δεδομένων. Ο *σημασιολογικός ιστός* (semantic web) περιλαμβάνει τη σαφή αναπαράσταση του νοήματος των πληροφοριών και των εγγράφων, επιτρέποντας την αυτόματη επεξεργασία και ενοποίηση διαδικτυακών πόρων από "έξυπνα" προγράμματα-πράκτορες. Ο σημασιολογικός ιστός θα επιτρέψει τον γρήγορο και ακριβή εντοπισμό πληροφοριών στον παγκόσμιο ιστό καθώς και την ανάπτυξη ευφυών διαδικτυακών πρακτόρων οι οποίοι θα διευκολύνουν την επικοινωνία μεταξύ πληθώρας ετερογενών ηλεκτρονικών συσκευών με πρόσβαση στο διαδίκτυο. Τα *συνδεδεμένα δεδομένα* (linked data) έχουν να κάνουν με την χρήση του Web για σύνδεση σχετιζόμενων δεδομένων που δεν ήταν προηγουμένως συνδεδεμένα ή την χρήση του Web για να περιοριστούν οι φραγμοί στα συνδεδεμένα δεδομένα που χρησιμοποιούν άλλες μεθόδους για την σύνδεση τους. [35] Πιο συγκεκριμένα η Wikipedia ορίζει τα συνδεδεμένα δεδομένα ως "μία μέθοδος για την δημοσίευση δομημένων δεδομένων, έτσι ώστε να μπορούν να διασυνδεθούν και να γίνουν πιο χρήσιμα για τους χρήστες".

Το ζήτημα προστασίας της ιδιωτικότητας έχει προκύψει σχετικά πρόσφατα, αρκεί να αναλογιστεί κανείς πως ο πρώτος νόμος περί προστασίας της ιδιωτικότητας θεσπίστηκε μόλις το 19^{ο} αιώνα στις Η.Π.Α. Τα πλαίσια της ιδιωτικότητας μεταβάλλονται διαρκώς. Οι λύσεις που θα προταθούν δεν θα πρέπει να είναι μόνο τεχνολογικής φύσεως. Απαιτείται σύνθετη αντιμετώπιση με συνδυασμό τεχνολογικών επιτευγμάτων και υιοθέτηση κατάλληλου ρυθμιστικού και νομικού πλαισίου. Επιπλέον προκύπτουν νέες προκλήσεις που αφορούν τρείς κύριους άξονες:

1. Το νομικό πλαίσιο θα πρέπει με δυναμικό τρόπο να μπορεί να προσαρμόζεται κατάλληλα στην τεχνολογία η οποία εξελίσσεται με τρομακτικά γρήγορους ρυθμούς. Συνήθως μεσολαβεί αρκετά μεγάλο χρονικό διάστημα από την στιγμή που προκύπτει η ανάγκη για την δημιουργία κάποιου νέου νόμου μέχρι την θέσπιση και την εφαρμογή του, οπότε τελικά να μην είναι πλέον επίκαιρος ή αναγκαίος καθώς η τεχνολογία έχει προχωρήσει ένα βήμα παραπέρα.
2. Οι ανάγκες και οι απαιτήσεις για ιδιωτικότητα διαφοροποιούνται ανάλογα με την ηλικία, τα άτομα και τους πολιτισμούς.
3. Θα πρέπει να δημιουργηθεί μια ενιαία πλατφόρμα η οποία με δυναμικό (dynamic) τρόπο θα μπορεί να προσαρμόζεται κατάλληλα ώστε να δίνει απαντήσεις στις νέες προκλήσεις που συνεχώς θα προκύπτουν, σε

συντεταγμένο επίπεδο από παγκόσμιους φορείς και όχι μόνο σε τοπικό επίπεδο.

Ο διάλογος για αυτά τα ζητήματα ξεπερνά τα όρια της τεχνολογίας και της νομοθεσίας. Οφείλουμε ως κοινωνία να προβληματιστούμε και να αναρωτηθούμε τι πραγματικά θέλουμε από αυτό που ονομάζουμε Κοινωνία της Πληροφορίας. Θα πρέπει επίσης να λάβουμε υπόψη μας την διαρκή διαμάχη ανάμεσα στις ατομικές απαιτήσεις ιδιωτικότητας και τις απαιτήσεις κρατικών και ιδιωτικών δομών. Επιπλέον οι χρήστες θα πρέπει να ευαισθητοποιηθούν και να ενημερωθούν όσο αφορά την προστασία της ιδιωτικότητας τους. Η ενημέρωση αυτή πρέπει να είναι προσβάσιμη από όλους, ακριβής και χωρίς περίπλοκους τεχνικούς όρους Η ανάλυση τέτοιων ζητημάτων ξεπερνά τους στόχους της παρούσας εργασίας.

Μέσα στα κοινωνικά πλαίσια τα οποία αναδιαμορφώνονται συνεχώς είναι προφανής η ανάγκη λύσεων δυναμικών και όχι στατικών. Το πρόβλημα χαρακτηρίζεται ως Ηράκλειτο καθώς τα δεδομένα του μεταβάλλονται συνεχώς. Οι λύσεις που θα προταθούν από την τεχνολογία θα πρέπει να κινούνται σε συμβιβαστικά πλαίσια καθώς καμιά λύση δεν μπορεί να είναι μόνιμη ή απόλυτη. Εισαγόμαστε σταδιακά σ' έναν κόσμο ρευστό με ότι αυτό συνεπάγεται. Οι τεχνολογικές εξελίξεις πραγματοποιούνται με τρομακτικά γρήγορο ρυθμό και οι επιστήμονες φαίνεται να προσπαθούν συνεχώς να τις προφτάσουν, π.χ. ποιος θα μπορούσε να φανταστεί τα προβλήματα ιδιωτικότητας που θα προέκυπταν αργότερα όταν πρωτοεμφανίστηκε το Facebook. Απώτερος στόχος λοιπόν είναι να είμαστε προετοιμασμένοι ώστε να ανακατευθύνουμε τις εξελίξεις της τεχνολογίας και όχι απλά να προσπαθούμε συνεχώς να διορθώνουμε τα "κακώς κείμενα" που θα προκύπτουν.

7 Αναφορές

[1] *Νέες καταγγελίες για παραβίαση προσωπικών δεδομένων στο Facebook* Διαθέσιμο στον δικτυακό τόπο: http://news.pathfinder.gr/scitech/681381.html (25/03/2011)

[2] *Πιέσεις ΕΕ προς Facebook για προστασία προσωπικών δεδομένων* (18/03/2011) Διαθέσιμο στον δικτυακό τόπο: http://www.mediasoup.gr/node/28381 (20/04/2011)]

[3] Φραγκάκης. Ν, 2008 *Τα όρια μεταξύ ελευθερίας και ασφάλειας, δημόσιου και ιδιωτικού,* Διαθέσιμο στην ιστοσελίδα της εφημερίδας «ΤΟ ΒΗΜΑ»: http://www.vimaideon.gr//Article.aspx?d=20080201&nid=7342365&sn=%CA%D5%D1%C9%CF%20%D4%C5%D5%D7%CF%D3&spid=1478&cs=1 (15/03/2011)

[4] *Information Privacy* Διαθέσιμο στον δικτυακό τόπο: http://en.wikipedia.org/wiki/Information_privacy (20/03/2011)

[5] *«Υφαρπαγή διευθύνσεων»: Για παραβίαση της ιδιωτικής ζωής κατηγορείται το Facebook στη Γερμανία* (07/07/2010) Διαθέσιμο στην ιστοσελίδα της εφημερίδας «ΤΟ ΒΗΜΑ»: http://www.tovima.gr/relatedarticles/article/?aid=341985 (12/05/2011)

[6] Stan Schroeder (2011), *France Fines Google $ 142,000 for Privacy Violations*, Διαθέσιμο στην ιστοσελίδα: http://mashable.com/2011/03/21/france-fine-google-street-view/ (25/05/2011)

[7] *Το iPhone δεν είναι συσκευή παρακολούθησης, επιμένει η Apple* (2011), Διαθέσιμο στην ιστοσελίδα: http://tech.in.gr/news/article/?aid=1231106844 (20/02/2011)

[8] K. Langley, *Cloud computing: Get your head in the clouds*, Διαθέσιμο στην ιστοσελίδα http://www.productionscale.com/home/2008/4/24/cloud-computing-get-your-head-in-the-clouds.html#axzz1MsYczIt3

[9] *Open Cloud Manifesto* Διαθέσιμο στην ιστοσελίδα του Open Cloud Manifesto: http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf (15/01/2011)

[10] John Horrigan (2009), *Wireless Internet Use*, Διαθέσιμο στην ιστοσελίδα: http://www.pewinternet.org/Reports/2009/12-Wireless-Internet-Use.aspx (20/01/2011)

[11] Steve Hamm (2009), *How Cloud Computer Will Change Business*, Διαθέσιμο στην ιστοσελίδα: http://www.businessweek.com/print/magazine/content/09_24/b4135042942270.htm (15/02/2011)

[12] IDC, *Press release: IDC finds more of the world's population connecting to the Internet in new ways and embracing Web 2.0 activities* Διαθέσιμο στην ιστοσελίδα: http://findarticles.com/p/articles/mi_m0EIN/is_2008_June_25/ai_n27507869/ (20/02/2011)

[13] Peter Mell & Tim Grance (2009), *The NIST Definition of Cloud Computing* Διαθέσιμο στην ιστοσελίδα: http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf (20/02/2011)

[14] Jinesh Varia (2008), *Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures* Διαθέσιμο στην ιστοσελίδα: http://aws.amazon.com/articles/1632/180-8035696-2121040 (21/02/2011)

[15] *Jeff Bezos' Risky Bet* (2007) Διαθέσιμο στην ιστοσελίδα http://www.businessweek.com/magazine/content/06_46/b4009001.htm(21/02/2011)

[16] B. Rochwerger, J. Caceres, R.S. Montero, D. Breitgand, E. Elmroth, A. Galis, E. Levy, I.M. Llorente, K. Nagin, Y. Wolfsthal, E. Elmroth, J. Caceres, M. Ben-Yehuda, W. Emmerich, F. Galan. "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4. (2009)

[17] Exploring the limits of cloud computing, V I C TO R D E LGADO Master of Science Thesis Stockholm, Sweden 2010

[18] *Virtualization* Διαθέσιμο στην ιστοσελίδα: http://en.wikipedia.org/wiki/Virtualization (12/02/2011)

[19] *Utility Computing* Διαθέσιμο στην ιστοσελίδα: http://en.wikipedia.org/wiki/Utility_computing (12/02/2011)

[20] Χρόνη Μ., Μποζιάρης Β., Νικολόπουλος Σ. (2010) *Πρόταση Χρήσης Τεχνολογίας Υπολογιστικού Νέφους στην Εκπαίδευση* Πρακτικά Εργασιών 7ου Πανελλήνιου Συνεδρίου με Διεθνή Συμμετοχή «Οι ΤΠΕ στην Εκπαίδευση», τόμος ΙΙ, σ. 35-44

[21] Katz, R (ed) (2009), *The Tower and the Cloud: Higher Education in the Age of Cloud Computing*, Διαθέσιμο στην ιστοσελίδα του Educause http://www.educause.edu/thetowerandthecloud (20/02/2011)

[22] Goldstein, P (2009), The Tower, the Cloud, and the IT leader and workforce, in Katz, R (ed) (2009), *The Tower and the Cloud: Higher Education in the Age of Cloud Computing*, Διαθέσιμο στην ιστοσελίδα του Educause http://www.educause.edu/thetowerandthecloud (20/02/2011)

[23] CLOUD COMPUTING: WHAT YOU SHOULD KNOW http://www.elctech.com/docs/ELC_Cloud_Computing_Gauide.pdf Ημερομηνία 26/08/2010

[24] Ismael Chang Ghalimi, (2010) *Benefits of Cloud Computing* Διαθέσιμο στην ιστοσελίδα http://www.intalio.com/html/documents/Benefits%20of%20Cloud%20Computing.pdf (25/02/2011)

[25*] Top Threats to Cloud Computing* (2010) V1.0 Prepared by the Cloud Security Alliance Διαθέσιμο στην ιστοσελίδα: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (02/03/2011)

[26] Armbrust, M et al (2009), *Above the clouds: A Berkeley view of Cloud Computing*, UC Berkeley EECS, Διαθέσιμο στην ιστοσελίδα: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (03/03/2011)

[27] *Chromebook Features* Διαθέσιμο στην ιστοσελίδα: http://www.google.com/chromebook/#features (08/06/2011)

[28] *Chrome OS Privacy Notice* Διαθέσιμο στην ιστοσελίδα: http://www.google.com/chromebook/#privacy(08/06/2011)

[29] *Identity Mixer*, Διαθέσιμο στην ιστοσελίδα: https://researcher.ibm.com/researcher/view_project.php?id=664 (05/05/2011)

[30] *Microsoft U-Prove Community Technology Preview R2* Διαθέσιμο στην ιστοσελίδα: https://connect.microsoft.com/site1188 (05/05/2011)

[31] *ABC4Trust - Project description* (2009), Διαθέσιμο στην ιστοσελίδα: http://www.computerworld.com.pt/media/2011/01/ABC4Trust-Project-Description.pdf (15/05/2011)

[32] European Network and Information Security Agency (2009), *Privacy Features of European eID Card Specifications* Διαθέσιμο στην ιστοσελίδα: www.enisa.europa.eu/act/it/eid/eid-cards-en (18/05/2011)

[33] Kim Cameron (2005) *The Laws of Identity* Διαθέσιμο στην ιστοσελίδα: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (20/05/2011)

[34] Ann Cavoukian *Privacy in the clouds* A White Paper on Privacy and Digital Identity: Implications for the Internet Διαθέσιμο στην ιστοσελίδα: http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf (20/05/2011)

[35] *Linked Data – Connect Distributed Data across the Web* Διαθέσιμο στην ιστοσελίδα: http://linkeddata.org/ (20/05/2011)